On the Eve of our President's Birthday : 30 June 2023

A Text Book on

Smart Grid Technology

Dr. K. Saravanan
Er. A. Raja
Dr. R. Sivanand
Dr. K. Senthilkumar

Department of Electrical & Electronics Engineering

Dr. M.G.R.
EDUCATIONAL AND RESEARCH INSTITUTE
DEEMED TO BE UNIVERSITY
University with Graded Autonomy Status
(An ISO 21001 : 2018 Certified Institution)
Periyar E.V.R. High Road, Maduravoyal, Chennai-95. Tamilnadu, India.

A Text Book on

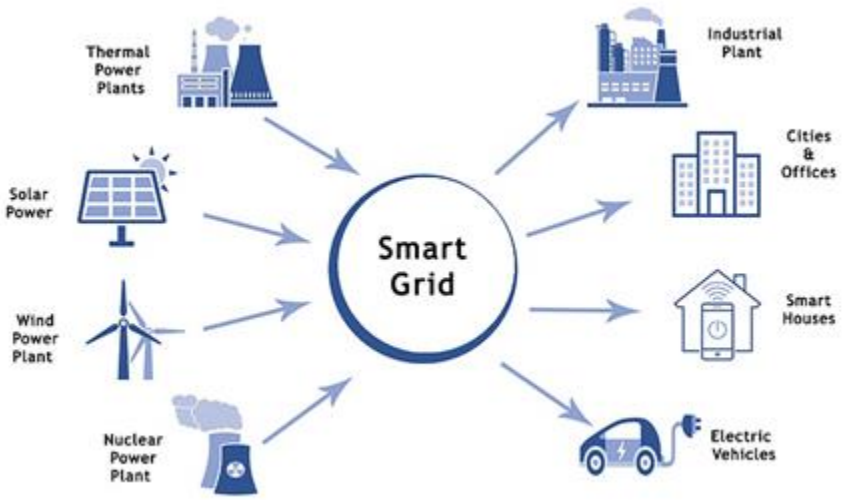
SMART GRID TECHNOLOGY

Dr. K. Saravanan

Er. A. Raja

Dr. R. Sivanand

Dr. K. Senthilkumar



Department of Electrical & Electronics Engineering

Dr. M.G.R.
EDUCATIONAL AND RESEARCH INSTITUTE
DEEMED TO BE UNIVERSITY
University with Graded Autonomy Status
(An ISO 21001 : 2018 Certified Institution)
Periyar E.V.R. High Road, Maduravoyal, Chennai-95. Tamilnadu, India.

A Text Book on

Smart Grid Technology

All rights are reserved. No part of the publication may be reproduced, stored in a retrieval system (including but not limited to computers, disks, external drives, electronic or digital devices, e-readers, websites), or transmitted in any form or by any means (including but not limited to cyclostyling, photocopying, docutech of other reprographic reproductions, mechanical, recording, electronic, digital versions) without the prior written permission of the publisher, not be otherwise circulated in any form of binding or cover other than that in which it is published and without a similar condition being imposed on the subsequent purchaser.

June 2023

Published by:

Department of Electrical & Electronics Engineering
Dr MGR Educational and Research Institute
[Deemed to be University]
Maduravoyal, Chennai - 600 095

Funded by:

Na Subbu Reddiar 100 Educational Trust
AD-13, 5th Street, Anna Nagar West, Chennai—600 040

978-93-95054-53-9

Printed at:

DJ Printers, Chennai – 600 095

CONTENTS

Unit 1: Introduction to Smart Grid ***1-48***

1.1 The Traditional Power Grid? *2*

1.1.1 Key Components *2*

1.1.2 Characteristics and Challenges *3*

1.1.3 Modernization Efforts *3*

1.2 Definitions: What's a Smart Grid? *3*

1.3 Why do we need a Smarter Grid? *5*

1.4 Smart Grid Risks *9*

1.5 Smart Grid Risks Versus Benefits *10*

1.5.1 Benefits of Smart Grids *10*

1.5.2 Risks of Smart Grids *11*

1.6 Regulations, Smart Grid and The Bulk Electric System *11*

1.7 National Smart Grid Mission – India *15*

1.7.1 Objective of NSGM *16*

1.7.2 NSGM Achievements *19*

1.7.3 Regulatory Authorities in Indian Power Sector *19*

1.8 Privacy Information Impacts on Smart Grid *20*

1.9 Security Standards *23*

1.10 Smart Grid Security Strategy *27*

1.11 Smart Grid Impacts *35*

1.12 Applying Security Control Framework to Smart Grid *38*

1.13 Managing the Overall Risk to Smart Grid *43*

Short and Long Answer Type Questions *47*

Unit 2: Smart Grid Communications and Measurement Technology ***49-64***

2.1 Communication and measurement *49*
2.1.1 Importance *50*
2.1.2 Local Area Network *51*
2.1.3 Home Access Network *52*
2.1.4 Neighborhood Area Network *52*
2.2 Monitoring ,PMU, Smart Meters and Measurements Technologies *53*
2.2.1 Wide Area Monitoring Systems (WAMS) *53*
2.2.2 Phasor Measurement Units (PMU) *54*
2.2.3 Smart Meters *55*
2.2.4 Smart Appliances *56*
2.2.5 Advanced Metering Infrastructure(AM0) *56*
2.3 GIS and Google Mapping Tools *57*
2.4 Multi Agent System (MAS)Technology *58*
2.4.1 Multiagent Systems for Smart Grid Implemetation *59*
2.4.2 Multiagent Specifications *59*
2.4.3 Multiagent Technique *60*
2.5 Microgrid and Smart grid Comparison *61*

Short and Long Answer Type Questions *63*

Unit 3: Pathway for Designing Smart Grid ***65-84***

3.1 Introduction To Smart Grid Pathway Design *65*
3.2 Barriers And Solutions To Smart Grid Development *67*
3.3 Solution Pathways For Designing Smart Grid Using Advanced Optimization And Control Techniques For Selection Functions *68*
3.4 General Level Automation *68*
3.4.1 Reliability *69*
3.4.2 Stability *69*
3.4.3 Economic Dispatch *71*
3.4.4 Unit Commitment (UC) *72*
3.4.5 Security Analysis *74*
3.5 Bulk Power Systems Automation of the smart grid at Transmission Level *74*
3.5.1 Fault and Stability Diagnosis *75*

3.5.2 Reactive Power Control 75

3.6 Distribution System Automation Requirement of the Power Grid 76

3.6.1 Voltage/VAr Control 76

3.6.2 Power Quality 78

3.6.3 Network Reconfiguration 80

3.6.4 Demand Side Management 80

3.6.5 Distribution Generation Control 81

3.7 End User/Appliance Level of The Smart Grid 81

3.8 Applications for Adaptive Control and Optimization 81

Short and Long Answer Type Questions 83

Unit 4: Renewable Energy and Storage 85-110

4.1 Renewable Energy Resources and Storage 85

4.2 Sustainable Energy Options For The Smart Grid 86

4.2.1 Solar Energy 86

4.2.2 Solar Power Technology 87

4.2.3 Modeling PV Systems 87

4.2.4 Wind Turbine Systems 90

4.2.5 Biomass-Bio energy 91

4.2.6 Small and Micro Hydropower 92

4.2.7 Fuel Cell 92

4.2.8 Geothermal Heat Pumps 93

4.3 Penetration And Variability Issues Associated With Sustainable Energy Technology 93

4.4 Demand Response Issues 95

4.5 Electric Vehicles and Plug-in Hybrids 96

4.6 PHEV Technology 96

4.6.1 Impact of PHEV on the Grid 97

4.7 Environmental Implications 98

4.7.1 Climate Change 98

4.7.2 Implications of Climate Change 98

4.8 Energy Storage Technologies 99

4.9 Types of Energy Storage Technologies 101

4.9.1 Batteries *101*
4.9.2 Flow Battery *102*
4.9.3 Fuel Cell and Hydrogen Electrolyser *104*
4.9.4 Flywheels *105*
4.9.5 Superconducting Magnetic Energy Storage Systems *107*
4.10 Tax Credits *107*
Short and Long Answer Type Questions *109*

Unit 5: Interoperability, Standards and Cyber Security ***111-124***
5.1 Introduction *111*
5.2 Interoperability *112*
5.2.1 State-of-the-Art-Interoperability *112*
5.2.2 Benefits and Challenges of Interoperability *113*
5.2.3 Model for Interoperability in the smart grid environment *113*
5.2.4 Smart Grid Network Interoperability *113*
5.2.5 Interoperability and Control of the Power Grid *114*
5.3 Standards *114*
5.3.1 Approach to Smart Grid Interoperability Standards *115*

5.4 Smart Grid Cyber Security *115*
5.4.1 Cyber Security State of the Art *116*
5.4.2 Cyber Security Risks *118*
5.4.3 Cyber Security Concerns Associated with AMI *120*
5.4.4 Mitigation Approach to Cyber Security Risks *120*

5.5 Cyber Security And Possible Operation For Improving Methodology For Other Users *121*
5.6 Case Study Of RER Integration *121*
5.6.1 Description of Smart Grid Activity *122*
5.6.2 Approach for Smart Grid Application *122*

Short and Long Answer Type Questions *124*

1 Introduction to Smart Grid

Established electric power systems, which have developed over the past 70 years, feed electrical power from large central generators up through generator transformers to a high voltage inter-connected network, known as the transmission grid. Each individual generator unit, whether powered by hydropower, nuclear power or fossil fuelled, is large with a rating of up to 1000 MW. The transmission grid is used to transport the electrical power, sometimes over considerable distances, and this power is then extracted and passed through a series of distribution transformers to final circuits for delivery to the end customers.

The part of the power system supplying energy (the large generating units and the transmission grid) has good communication links to ensure its effective operation, to enable market transactions, to maintain the security of the system, and to facilitate the integrated operation of the generators and the transmission circuits. This part of the power system has some automatic control systems though these may be limited to local, discrete functions to ensure predictable behaviour by the generators and the transmission network during major disturbances.

The distribution system, feeding load, is very extensive but is almost entirely passive with little communication and only limited local controls. Other than for the very largest loads (for example, in a steelworks or in aluminium smelters), there is no real-time monitoring of either the voltage being offered to a load or the current being drawn by it. There is very little interaction between the loads and the power system other than the supply of load energy whenever it is demanded.

The present revolution in communication systems, particularly stimulated by the internet, offers the possibility of much greater monitoring and control throughout the power system and hence more effective, flexible and lower cost operation. The Smart Grid is an opportunity to use new ICTs (Information and Communication Technologies) to revolutionise the electrical power system. However, due to the huge size of the power system and the scale of investment that has been made in it over the years, any significant change will be expensive and requires careful justification.

The consensus among climate scientists is clear that man-made greenhouse gases are leading to dangerous climate change. Hence ways of using energy more effectively and generating electricity without the production of CO2 must be found. The effective management of loads and reduction of losses and wasted energy needs accurate information while the use of large amounts of renewable generation requires the integration of the load in the operation of the power system in order to help balance supply and demand. Smart meters are an important element of the Smart Grid as they can provide information about the loads and hence the power flows throughout the network. Once all the parts of the power system are monitored, its state becomes observable and many possibilities for control emerge.

In the UK, the anticipated future de carbonised electrical power system is likely to rely on generation from a combination of renewables, nuclear generators and fossil-fuelled plants with carbon capture and storage. This combination of generation is difficult to manage as it consists of variable renewable generation and large nuclear and fossil generators with carbon capture and storage that, for technical and commercial reasons, will run mainly at constant output. It is hard to see how such a power system can be operated cost-effectively without the monitoring and control provided by a Smart Grid.

1.1 THE TRADITIONAL POWER GRID

The traditional power grid, also known as the electrical grid or the utility grid, refers to the network of power generation, transmission, and distribution infrastructure that delivers electricity from power plants to consumers. It is the system that provides electrical power to homes, businesses, and industries.

1.1.1 Key Components:

1. Power Generation: Power plants, such as coal-fired, natural gas, nuclear, hydroelectric, and renewable energy facilities, produce electricity by converting various energy sources into electrical energy.
2. Transmission System: High-voltage transmission lines transport electricity over long distances from power plants to local areas. These lines are usually mounted on tall towers or poles to minimize transmission losses.
3. Substations: Substations act as distribution centers and transfer electricity from high-voltage transmission lines to lower-voltage distribution lines. They also include transformers that step down the voltage for local distribution.
4. Distribution System: The distribution system consists of a network of lower-voltage power lines, transformers, and other equipment that distribute electricity to end-users, including

homes, businesses, and industrial facilities.

5. Consumer Connection: Electricity is finally delivered to consumers through power lines and electrical connections in buildings, allowing them to access and use electrical power for various purposes.

1.1.2 Characteristics and Challenges:

1. Centralized Generation: Traditional power grids typically rely on large, centralized power plants that generate electricity at a few key locations. This centralized generation model can pose challenges in terms of efficiency, reliability, and environmental impact.
2. Unidirectional Flow: The power grid follows a unidirectional flow of electricity, where power is generated at the source and delivered to consumers without significant feedback or interaction between consumers and the grid.
3. Grid Vulnerability: Traditional power grids are vulnerable to disruptions such as natural disasters, equipment failures, and cyber attacks. These vulnerabilities can lead to widespread power outages and significant economic and social impacts.
4. Limited Storage: The traditional grid has limited energy storage capacity, making it challenging to balance supply and demand in real-time. This limitation becomes more critical with the increasing integration of intermittent renewable energy sources.

1.1.3 Modernization Efforts:

In recent years, there have been efforts to modernize and transform the traditional power grid into a more resilient, flexible, and sustainable system. These efforts include:

1. Smart Grid Technology
2. Distributed Generation
3. Energy Storage:
4. Microgrids
5. Renewable Energy Integration

1.2 DEFINITIONS: WHAT'S A SMART GRID?

The Smart Grid concept combines a number of technologies, end-user solutions and addresses a number of policy and regulatory drivers. It does not have a single clear definition.

The European Technology Platform defines the Smart Grid as:

"*A SmartGrid is an electricity network that can intelligently integrate the actions of all users connected to it – generators, consumers and those that do both – in order to efficiently deliver sustainable, economic and secure electricity supplies.*"

According to the US Department of Energy :

"*A smart grid uses digital technology to improve reliability, security, and efficiency (both economic and energy) of the electric system from large generation, through the delivery systems to electricity consumers and a growing number of distributed-generation and storage resources.*"

In *Smarter Grids: The Opportunity* , the Smart Grid is defined as:

"*A smart grid uses sensing, embedded processing and digital communications to enable the electricity grid to be observable (able to be measured and visualised), controllable (able to manipulated and optimised), automated (able to adapt and self-heal), fully integrated (fully interoperable with existing systems and with the capacity to incorporate a diverse set of energy sources).*"

The literature suggests the following attributes of the Smart Grid:

1. It enables demand response and demand side management through the integration of smart meters, smart appliances and consumer loads, micro-generation, and electricity storage (electric vehicles) and by providing customers with information related to energy use and prices. It is anticipated that customers will be provided with information and incentives to modify their consumption pattern to overcome some of the constraints in the power system.
2. It accommodates and facilitates all renewable energy sources, distributed generation, residential micro-generation, and storage options, thus reducing the environmental impact
3. of the whole electricity sector and also provides means of aggregation. It will provide simplified interconnection similar to 'plug-and-play'.
4. It optimises and efficiently operates assets by intelligent operation of the delivery system (rerouting power, working autonomously) and pursuing efficient asset management. This includes utilising asserts depending on what is needed and when it is needed.
5. It assures and improves reliability and the security of supply by being resilient to disturbances, attacks and natural disasters, anticipating and responding to system disturbances (predictive maintenance and self-healing), and strengthening the security of supply through enhanced transfer capabilities.
6. It maintains the power quality of the electricity supply to cater for sensitive equipment that increases with the digital economy.
7. It opens access to the markets through increased transmission paths, aggregated supply and demand response initiatives and ancillary service provisions

As Figure 1.1 depicts, the traditional electrical grid is very hierarchical, with generation at the top, transmission in the middle, and distribution at the bottom operating somewhat autonomously. Under the Smart Grid model, traditional generation still has a large role, but it is augmented by distributed generation in the form of wind, solar, and various other customer owned generation sources that not only generate electricity for the end customers, but can also sell electricity back to the utility. Additionally, communications networks are added to not only support distributed generation, but also to integrate customer interaction into the equation so utilities can both influence behavior and make better planning decisions based on customer choices. This includes technologies such as advanced metering infrastructure (AMI) that allow smart meters on houses and buildings to relay in near real-time the usage level of that facility. And through appliance-based communications technologies, grid components can even relay appliance level usage information and receive commands from the utility to alter the behavior or ultimate operation of the appliance during times of heavy electricity usage. In addition to distributed generation and enhanced communications and measurement capabilities, the Smart Grid also envisions the ability to store electricity for later usage via conventional and evolving battery technologies, compressed air, and pumped storage where water is pumped uphill during off-peak periods and then allowed to run down- hill during peak periods to generate electricity. One particularly interesting storage solution is the plug-in hybrid electric vehicle (PHEV) that is capable of both generating and storing electricity through a gasoline engine and battery and can also receive its energy from the electric grid by plugging it in using technology already available. The same technology could then be extended to allow these vehicles to store energy for later use by other devices on the electrical grid when not needed by the vehicle. It is this smoothing out of energy usage to maximize the generating capacity that is one of the key features of the Smart Grid.

1.3 WHY DO WE NEED A SMARTER GRID?

As has been mentioned already, the Smart Grid is not intended to fix problems with the current electrical grid. With a few exceptions in warm climates with heavy population such as Florida and Southern California, electricity is plentiful, reliable, and cheap. However, that is likely to change for a variety of reasons. In his book entitled Visions for a Sustainable Energy Future, Mark Gabriel highlights a variety of trends that are affecting our ability to stick with the status quo.

Traditional Grid Smart Grid

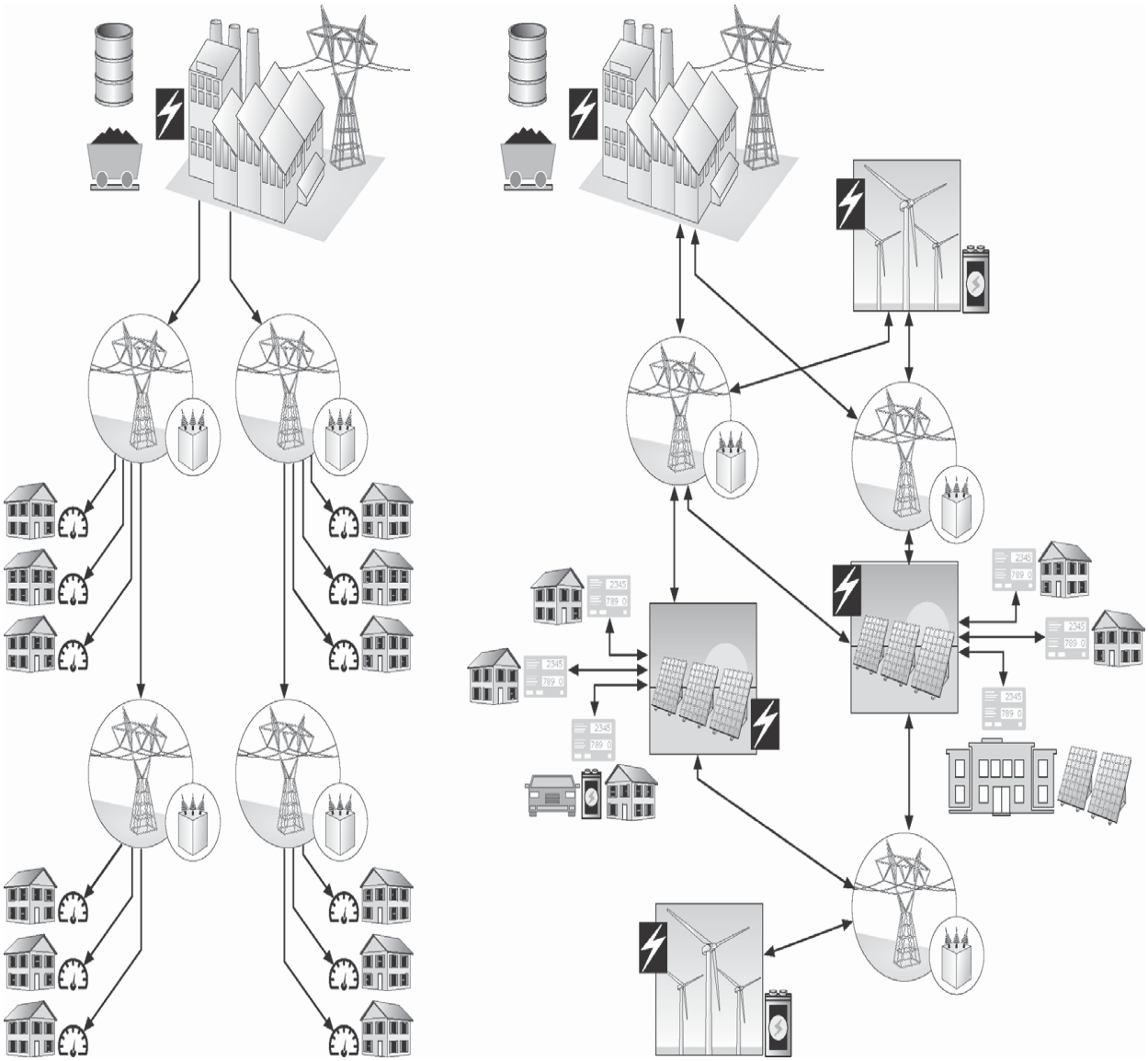


FIGURE 1.1 Traditional and Smart Grids

They include demographics, the evolution of the energy business, carbon constraints and capacity demands, availability of intelligent infrastructure, and the need for customer engagement. One could argue that the primary driver, however, is economic, and so, if investor owned utilities cannot make a profit or if electricity prices are too high for consumers, then change will be required. The reality is that multiple factors are driving this economic necessity. Demographic changes have driven more people to warm weather climates that demand more electricity for air conditioning, usually the largest single electricity cost when it is

used for residential purposes. Our electronic culture, from cell phones that need charging to large televisions that draw more electricity than a previous generation, is also increasing demand. And, of course, the supply side is also facing challenges from environmental regulations that restrict traditional fossil fuel-based generation plants, from very long and heavily regulated deployment windows for nuclear, and from the investment costs and long payback period for renewables such as solar and wind. These supply-and-demand challenges alone will likely cause dramatic increases in electricity costs, particularly in large population centers in warm climates. Additionally, electric utilities face an aging workforce with no ready replacements. Both the reality of fewer people to do the work and the preference of the younger generation to rely more on technology are driving utilities to embrace automation and outsourcing, which are not always very well thought out.

Despite being Fortune 500 companies in many cases, large investor- owned utilities face heavy regulation by public utility commissions over what they can charge their customers at the distribution level, and there- fore they are constantly searching for greater cost efficiencies and new markets to enter that are less regulated in order to keep investors interested. Taking advantage of the tax benefits, grants, and greater market orientation available on the generation side are some of the reasons to pursue renewable energy businesses. The DOE Smart Grid grants funded under the American Recovery and Reinvestment Act of 2009 gave some of these utilities an impetus when the economics in favor of Smart Grid investments were still a bit tenuous. More than that, Smart Grid presents a host of business opportunities and technological innovations in an industry that is not historically known for either. Customer engagement, while a bit less compelling, is one of these opportunities, along with the availability of a technology that creates its own demand. What may never have been on the radar of consumers and the public utility com- missions that represent them suddenly will become an imperative once easy and useful technologies are available. We never knew we needed cell phones or digital video recorders until they became economical and packaged for consumers. Now they are practically necessities.

The expected benefits for Smart Grid sound a bit anticlimactic when one first looks at the upfront investment. Most experts believe that energy prices will be higher regardless, but through Smart Grid, they will not go up as much. Consumers are likely to experience fewer rolling blackouts as utilities will be able to use demand response programs to turn off selected appliances during peak periods. And consumers will have more control over which appliances are turned off. While Smart Grid promises to reduce some outages through better predictive failure analytics and get help to reduce the duration of outages through near- immediate

pinpointing of customers without power, or at least meter connectivity, the Smart Grid will not do much to keep that big old tree from snapping the power lines to one's home during the next storm. Someday, distributed generation and localized energy storage may help Mitigate some of the storm-related outages. However, most homes are still likely to have single points of failure where trees and backhoe cuts still pose a danger.

As a business proposition, Smart Grid presents some of the same challenges as cyber security as the savings may be in costs avoided. Given the fairly low electricity rates that most Americans enjoy, the biggest savings will likely come from rates that will not go up as high as they would have otherwise, because as demand for energy increases, some rate increases are inevitable. Consequently, the savings that Smart Grid offers come from cost savings from lower staffing levels through greater automation, smaller revenue losses as a result of shorter outages, and lower generation costs through demand response and dynamic pricing programs that shift usage to lower demand time periods. There are many more Smart Grid use cases that could result in lower costs and fewer revenue losses. However, there are many unknowns. For example, demand response programs depend heavily on customer participation and changes in their behaviors. Savings from greater automation depend on achieving lower employee head counts. And the ability to shorten outages assumes that future outages will be easier to predict and faster to remedy with more advanced but still unproven technology. Added to this is the cost associated with the Smart Grid upgrade. Government subsidies through the American Recovery and Reinvestment Act are helping to ease that burden, but in many cases, utilities are seeking to pass the remaining costs to ratepayers, a proposition that is not going over well with public utilities commissions. Nonetheless, the electrical grid is sorely in need of investment. The only question is whether Smart Grid deployments will allow utilities to delay or avoid replacement of aging infrastructure, or if transformers and other grid workhorses at the end of their lives will demand replacement sooner rather than later.

The future grid is difficult to predict as so many factors come into play. Looking 50 years ahead, one can envision a highly dynamic distribution grid where individual consumers generate their own power through solar and wind and have storage and other resources to draw from when the sun does not shine or the wind is not blowing. Total electric usage will inevitably grow as we grow more reliant on technology and significant loads, such as plug-in hybrid electric vehicles, are added.

1.4 SMART GRID RISKS

While smart grids offer numerous benefits, there are also risks associated with their implementation. Some of the key risks of smart grids include:

1. Cyber security Threats: Smart grids heavily rely on digital communication networks, which increases the risk of cyber attacks. Hackers could potentially target and disrupt the grid, leading to power outages or other disruptions. It is crucial to implement robust cybersecurity measures to protect against unauthorized access, data breaches, and system manipulation.
2. Privacy Concerns: Smart grids collect vast amounts of data about energy consumption patterns, which can be sensitive and personally identifiable. There is a risk that this data could be compromised or misused, leading to privacy breaches. It is essential to establish strong privacy protections and ensure secure handling and storage of consumer data.
3. Interoperability and Standardization Challenges: Smart grid technologies involve multiple interconnected devices and systems from various manufacturers. Ensuring compatibility, interoperability, and standardization among these diverse components can be a challenge. Lack of standardized protocols may hinder effective communication and integration of different elements within the smart grid.
4. System Complexity and Integration: Smart grids introduce additional complexity to the power system due to the integration of various technologies, such as advanced metering infrastructure, communication networks, distributed energy resources, and demand response systems. Managing and coordinating these interconnected components require sophisticated control systems and can present challenges in terms of design, implementation, and operation.
5. Power Outage Dependency: The reliance on digital communication and control systems in smart grids means that a disruption or failure in these systems can potentially lead to power outages. It is crucial to have backup systems and redundancy measures in place to minimize the impact of such failures.
6. Regulatory and Policy Challenges: The deployment of smart grids involves navigating complex regulatory frameworks and addressing policy issues. Balancing the interests of different stakeholders, ensuring fair pricing and access to grid services, and establishing effective governance structures can be challenging.
7. Cost and Financial Considerations: Implementing smart grid technologies can require significant upfront investments. The cost of deploying advanced metering infrastructure, communication networks, and other components needs to be carefully evaluated and balanced against the potential benefits.

To mitigate these risks, it is essential to adopt robust cybersecurity measures, prioritize privacy protection, establish industry standards and protocols, conduct rigorous testing and validation, and ensure effective regulatory frameworks and policies are in place. Additionally, ongoing monitoring, threat assessments, and regular updates to security measures are vital to keep pace with evolving risks

1.5 SMART GRID RISKS VERSUS BENEFITS

With the Smart grids offer numerous benefits, but they also come with certain risks. Let's compare the risks and benefits of smart grids:

1.5.1 Benefits of Smart Grids:

1. Enhanced Energy Efficiency: Smart grids enable better monitoring and management of energy consumption, allowing consumers to make informed decisions about their energy usage. This promotes energy efficiency, reduces waste, and lowers electricity bills.
2. Integration of Renewable Energy: Smart grids facilitate the integration of renewable energy sources, such as solar and wind, by managing their intermittent generation and decentralized nature. This helps optimize their utilization and reduces grid instability.
3. Improved Reliability and Resilience: Smart grid technologies enhance the reliability and resilience of the power grid by enabling quick detection, isolation, and restoration of faults. This reduces downtime, improves power quality, and enhances the grid's ability to withstand disturbances or outages.
4. Better Grid Management: Smart grids provide real-time data and analytics, enabling grid operators to have a more comprehensive view of the system. This allows for better monitoring, control, and optimization of grid operations, leading to more efficient power distribution and load balancing.
5. Demand Response and Load Management: Smart grids support demand response programs, where consumers can adjust their energy usage based on price signals or grid conditions. This helps balance supply and demand, reduce peak loads, and avoid the need for additional power generation capacity.
6. Electric Vehicle Integration: Smart grids can support the charging infrastructure for electric vehicles (EVs) and manage the load on the grid. They enable efficient charging, promote the adoption of EVs, and contribute to reducing greenhouse gas emissions from transportation.

1.5.2 Risks of Smart Grids:

1. Cyber security Threats: Smart grids increase the risk of cyber attacks, potentially leading to power outages or grid disruptions. Adequate cyber security measures must be in place to protect against unauthorized access, data breaches, and system manipulation.
2. Privacy Concerns: The collection and analysis of vast amounts of consumer data by smart grids raise privacy concerns. There is a risk of data breaches or misuse of sensitive personal information. Strict privacy protections and secure data handling practices are necessary to address these concerns.
3. Interoperability and Standardization Challenges: The integration of diverse components from different manufacturers can pose challenges in terms of compatibility, interoperability, and standardization. Lack of standardized protocols may hinder effective communication and integration within the smart grid.
4. Complexity and Integration Issues: Smart grids introduce additional complexity to the power system, requiring sophisticated control systems. Designing, implementing, and operating interconnected technologies can be challenging.
5. Power Outage Dependency: Reliance on digital communication and control systems in smart grids means that failures or disruptions in these systems can result in power outages. Backup systems and redundancy measures are needed to minimize the impact of such failures.
6. Cost Considerations: Implementing smart grid technologies requires significant upfront investments. The cost of deploying advanced metering infrastructure, communication networks, and other components must be carefully evaluated against potential benefits.

While the risks associated with smart grids should not be ignored, many of these risks can be mitigated through proper planning, robust cyber security measures, privacy protections, standardized protocols, and ongoing monitoring and updates. When implemented effectively, the benefits of smart grids can outweigh the risks, leading to a more efficient, reliable, and sustainable electrical grid.

1.6 REGULATIONS, SMART GRID, AND THE BULK ELECTRIC SYSTEM

The Federal Energy Regulatory Commission (FERC) is an independent agency that regulates the interstate transmission of electricity, natural gas, and oil. The Energy Policy Act of 2005 provided FERC with additional responsibilities, to include the authority to regulate the transmission and wholesale sales of electricity in interstate commerce, licensing and inspection of private, municipal, and state hydroelectric projects, protecting the reliability of the high voltage interstate transmission system through mandatory reliability standards, monitoring and

investigating energy markets, and enforcing FERC regulatory requirements through imposition of civil penalties and other means. FERC does not specifically regulate retail electricity and natural gas sales to consumers, regulate nuclear power plants, or maintain oversight for problems related to the failures of local distribution facilities. These facts are key to understanding why the North American Electric Reliability Corporation (NERC) only has regulatory authority over the bulk electric system. NERC's primary mission is to ensure the reliability of the North American bulk power system. NERC is the electric reliability organization (ERO) certified by FERC to establish and enforce reliability standards for the bulk power system. "NERC develops and enforces reliability standards; monitors the bulk power system; and educates, trains and certifies industry personnel

It is important to understand that NERC is a non-profit corporation established to carry out and execute the regulatory obligations of FERC. This responsibility is vested in the fact that NERC has been established as the ERO, which provides them with the ability to enforce reliability standards. The reliability standards must be approved by FERC and, upon such approval, NERC is able to execute its mission. The NERC Critical Infrastructure Protection (NERC CIP) reliability standards were then developed to provide a means of measuring and managing the cyber security posture of the bulk electric system. Under FERC Order 706, NERC was given responsibility for developing the CIP standards as a method of executing FERC's regulatory responsibilities. As the task of ensuring that the CIP and other reliability standards are appropriately executed, NERC leverages regional entities. These regional entities include investor-owned utilities; federal power agencies; rural electric cooperatives; state, municipal, and provincial utilities; independent power producers; power marketers; and end use customers. The entities include (Figure 1.2)

- Florida Reliability Coordinating Council (FRCC)
- Midwest Reliability Organization (MRO)
- Northeast Power Coordinating Council (NPCC)
- Reliability First Corporation (RFC)
- SERC Reliability Corporation (SERC)
- Southwest Power Pool (SPP)
- Texas Reliability Entity (TRE)
- Western Electricity Coordinating Council (WECC)

The regional entities execute their responsibilities through compliance audits. NERC CIP and other reliability standards are broken down into a methodical format. You can expect the purpose to be clearly stated for each standard. Each standard also comes with an applicability clause that illustrates the responsibility entities that are on the hook for meeting the standards.

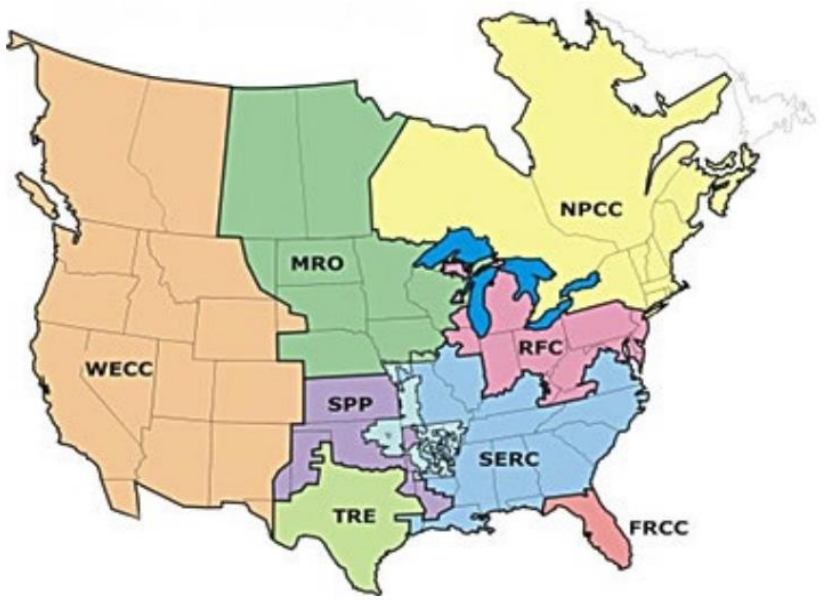


FIGURE 1.2 NERC regional entities.

The following list represents the list of responsible entities that are required to at least review the CIP 002 NERC CIP standard in order to determine whether or not they need to comply with the remainder of the standards (003-009):

- Reliability coordinator
- Balancing authority
- Interchange authority
- Transmission service provider
- Transmission owner
- Transmission operator
- Generation owner
- Generation operator
- Load-serving entity
- NERC
- Regional entity

The reliability coordinator is responsible for the reliable operation of the bulk electric system, has the wide area view of the bulk electric system, and has the operating tools, processes, and procedures, including the authority to prevent or mitigate emergency operating situations in both next-day analysis and real-time operations. A balancing authority "integrates resource plans ahead of time, maintains load-interchange- generation balance within a balancing authority area, and supports interconnection frequency in real time." The interchange authority "authorizes the implementation of valid and balanced Interchange schedules between balancing authority areas, and ensures communication of interchange information for reliability assessment purposes. A transmission service provider "administers the transmission tariff and provides transmission service to transmission customers under applicable transmission service agreements." A transmission owner "owns and maintains transmission facilities." Transmission operators are "responsible for the reliability of their 'local' transmission system, and are responsible for directing the operations of transmission facilities." A generation owner "owns and maintains generation facilities." Generation operators "operate generating unit(s) and perform the functions of supplying energy and Interconnected Operations Services." A load serving entity "secures energy and transmission service (and related interconnected operations services) to serve the electrical demand and energy requirements of its end-use customers." NERC and the regional entities are also required to review this standard.

All of these functions identified by NERC in the CIP standards rep- resent the functions required to manage and maintain the bulk electric system. This is primarily because the bulk electric system requires a high degree of communication and coordination among different utilities. Utilities then typically do not see themselves as competitors with each other, but rather as partners in the management of the bulk electric system. The CIP 002 standard is then used by entities that meet the criteria listed above to determine if they will need comply with the NERC CIP standards. The requirements listed in CIP 002 illustrate the process that must be executed in order to accomplish this task. Each entity is then required to declare assets within its area of responsibility as either critical or not critical, depending on the results of the execution of its compliant methodologies. Once an asset is declared critical, the entity must deter- mine if any cyber-assets are critical. If critical cyber-assets are identified, then the remainder of the CIP standards become applicable. Each entity with critical cyber-assets is then subjected to audits by the applicable regional entity. The regional entity utilizes the measurements found in the standards documentation to measure compliance with the standards. NERC goes further in refining what these measurements are through the development of "Reliability Standard Audit Worksheets," which are used as the checklist to determine compliance.

The manner in which NERC CIP is set up is important because it illustrates the process by which the cyber security infrastructure will be implemented for part of Smart Grid. NERC CIP is really the foundation on which utility companies are building out their security practices. This is mostly because the framework is well understood and familiar to utilities. It is important to note, however, that these standards do not apply to other parts of Smart Grid, mostly because FERC has no regulatory responsibilities as associated with the delivery of local and retail power. The compliance framework should also not be confused with the mechanism to secure the bulk electric system, but rather it is the infrastructure that will facilitate security. Because of this, many utilities will implement personnel and systems to augment compliance that will ultimately lead to cyber security practices.

In 2007, the Energy Independence and Security Act of 2007 was passed; it called for the "optimization of grid operations and resources, with full cyber security." As a result, Smart Grid efforts were meant to ramp up. But the most important component of this legislation called for the implementation of full cyber security during grid optimization or during the implementation of Smart Grid systems and services. This law then provides the legal justification for all utility companies that wish to implement Smart Grid components to ensure that they were implementing cyber security into their Smart Grid program life cycles. The key term "full cyber security" has not been clearly defined but it is likely being interpreted through the distribution of stimulus funding under the American Recovery and Reinvestment Act (ARRA). The ARRA requires utilities that have accepted Smart Grid funding for approved projects to implement cyber security into the life cycle of their projects. While no formal regulation such as NERC CIP has been established for these efforts, the requirements are forcing utility companies to develop cyber security programs to deal with this. From a strategic perspective, it is having the effect of integrating cyber security into the Smart Grid.

As these Smart Grid projects broaden and utilities undertake efforts to implement new Smart Grid components, cyber security will more than likely be addressed at some level.

1.7 National Smart Grid Mission - INDIA

National Smart Grid Mission (NSGM) was established in the Indian Power sector to plan and monitor the implementation of policies and programmes related to Smart Grid activities in India. It's an institutional mechanism for planning, monitoring and implementation of policies and programs related to Smart Grid activities. NSGM is housed under Ministry of Power (MoP) considering the fact that most of the prominent stakeholders (DISCOMS. Regulators, Electrical manufactures, Central Electricity Authority

etc.) for Smart Grid are associated with MoP. Other concerned Ministries like Ministry of New and Renewable Energy (MNRE), Ministry of Urban Development (MoUD) and Ministry of Heavy Industry (MoHl) are also associated with the Mission.

1.7.1 Objective of NSGM

National Smart Grid Mission was launched with an objective to address key issues of Smart Grid Initiatives on a large scale in the country and to make the Indian Power infrastructure cost effective, responsive and reliable. A 20 year perspective Plan for integrated inter-regional, inter- state and intra-state transmission network for the country as whole has been formulated. This will be a crucial backbone for the vision of 24x7power for all homes in India.

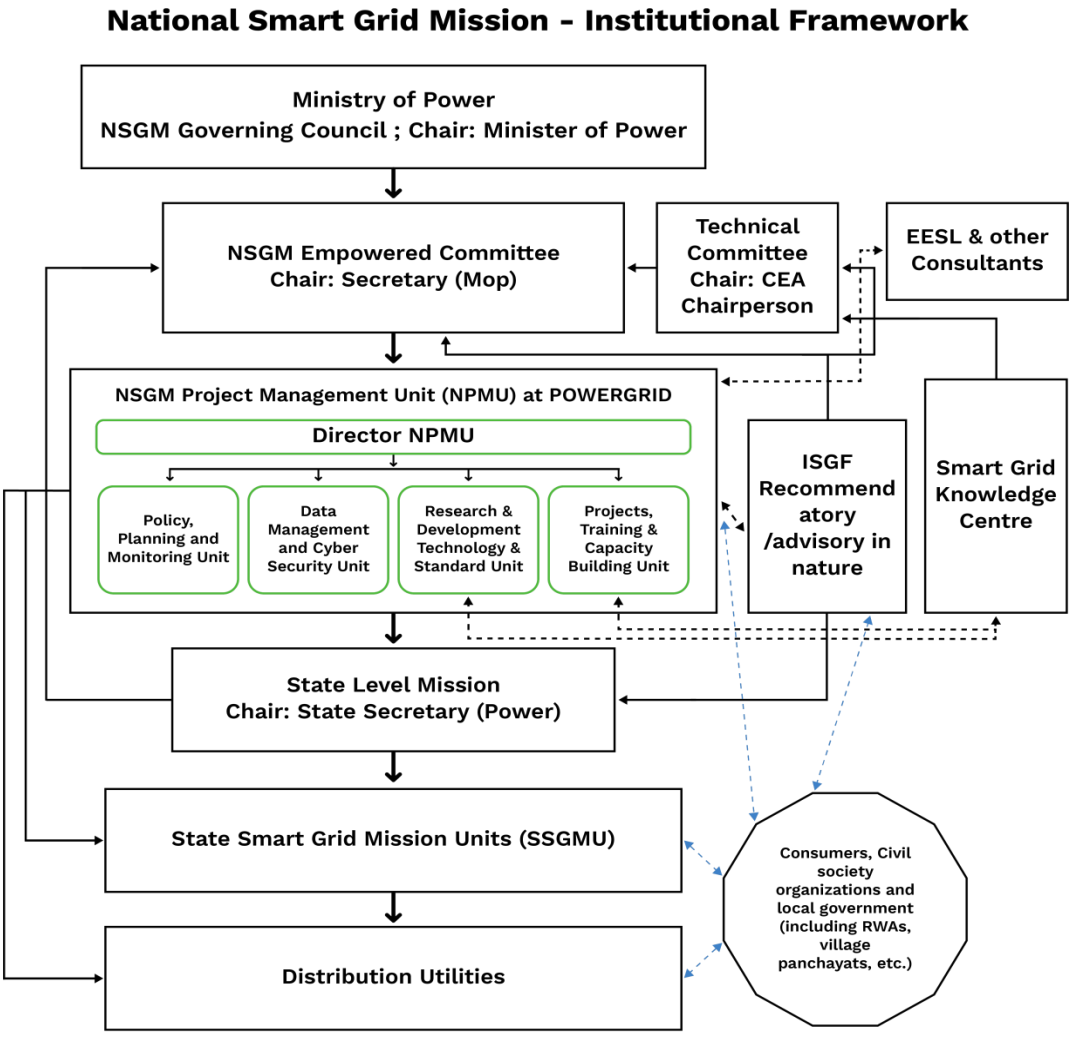

National Smart Grid Mission - Institutional Framework
Ministry of Power
NSGM Governing Council ; Chair: Minister of Power
NSGM Empowered Committee
Chair: Secretary (Mop)
Technical Committee
Chair: CEA
Chairperson
EESL & other Consultants
NSGM Project Management Unit (NPMU) at POWERGRID
Director NPMU
Policy, Planning and Monitoring Unit
Data Management and Cyber Security Unit
Research & Development Technology & Standard Unit
Projects, Training & Capacity Building Unit
ISGF Recommend atory /advisory in nature
Smart Grid Knowledge Centre
State Level Mission
Chair: State Secretary (Power)
State Smart Grid Mission Units (SSGMU)
Distribution Utilities
Consumers, Civil society organizations and local government (including RWAs, village panchayats, etc.)

FIGURE 1.3 - Tier 1

NSGM consists of a 3 tier structure:

Tier 1 (FIGURE 1.3)

At the apex level, NSGM is having a Governing Council headed by the Minister of Power. The Governing Council have necessary functional and financial autonomy within the overall budgetary allocation for meeting its objective of rolling out Smart Grid operations in different parts of the country. The detailed structure is depicted pictorially as below.

Tier 2 (FIGURE 1.4)

At the second level, the NSGM has an Empowered Committee headed by Secretary (Power). This level is responsible for the necessary budgetary and project approvals and the recruitment of consultants related to the projects. The detailed structure is depicted pictorially as below:

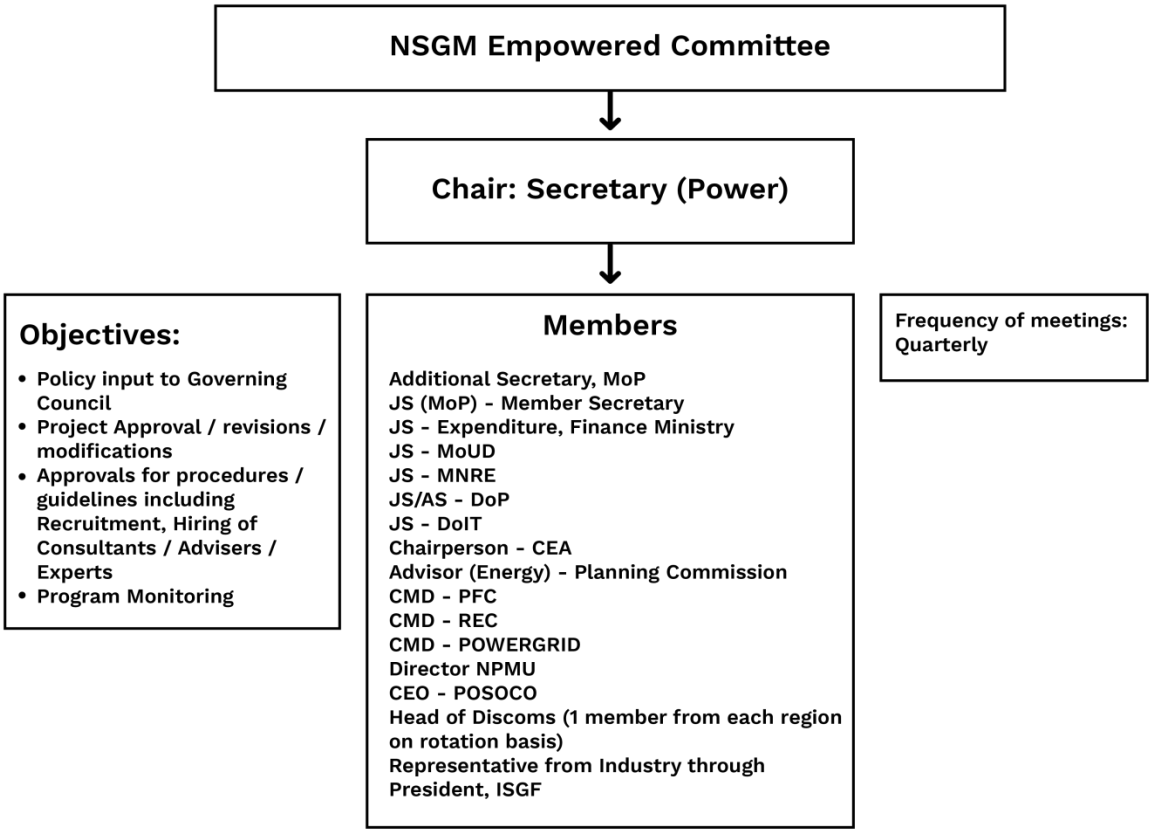

NSGM Empowered Committee
Chair: Secretary (Power)
Objectives:
• Policy input to Governing Council
• Project Approval / revisions / modifications
• Approvals for procedures / guidelines including Recruitment, Hiring of Consultants / Advisers / Experts
• Program Monitoring
Members
Additional Secretary, MoP
JS (MoP) - Member Secretary
JS - Expenditure, Finance Ministry
JS - MoUD
JS - MNRE
JS/AS - DoP
JS - DoIT
Chairperson - CEA
Advisor (Energy) - Planning Commission
CMD - PFC
CMD - REC
CMD - POWERGRID
Director NPMU
CEO - POSOCO
Head of Discoms (1 member from each region on rotation basis)
Representative from Industry through President, ISGF
Frequency of meetings: Quarterly

FIGURE 1.4 - Tier 2

Tier 3 (FIGURE 1.5)

There is a NSGM Technical Committee headed by Chairperson (CEA) which assumes a supporting role. Technical Committee supports the Empowered Committee on technical side and is responsible for on ground technology selection, standards development and technical review of various projects, activities and documents.

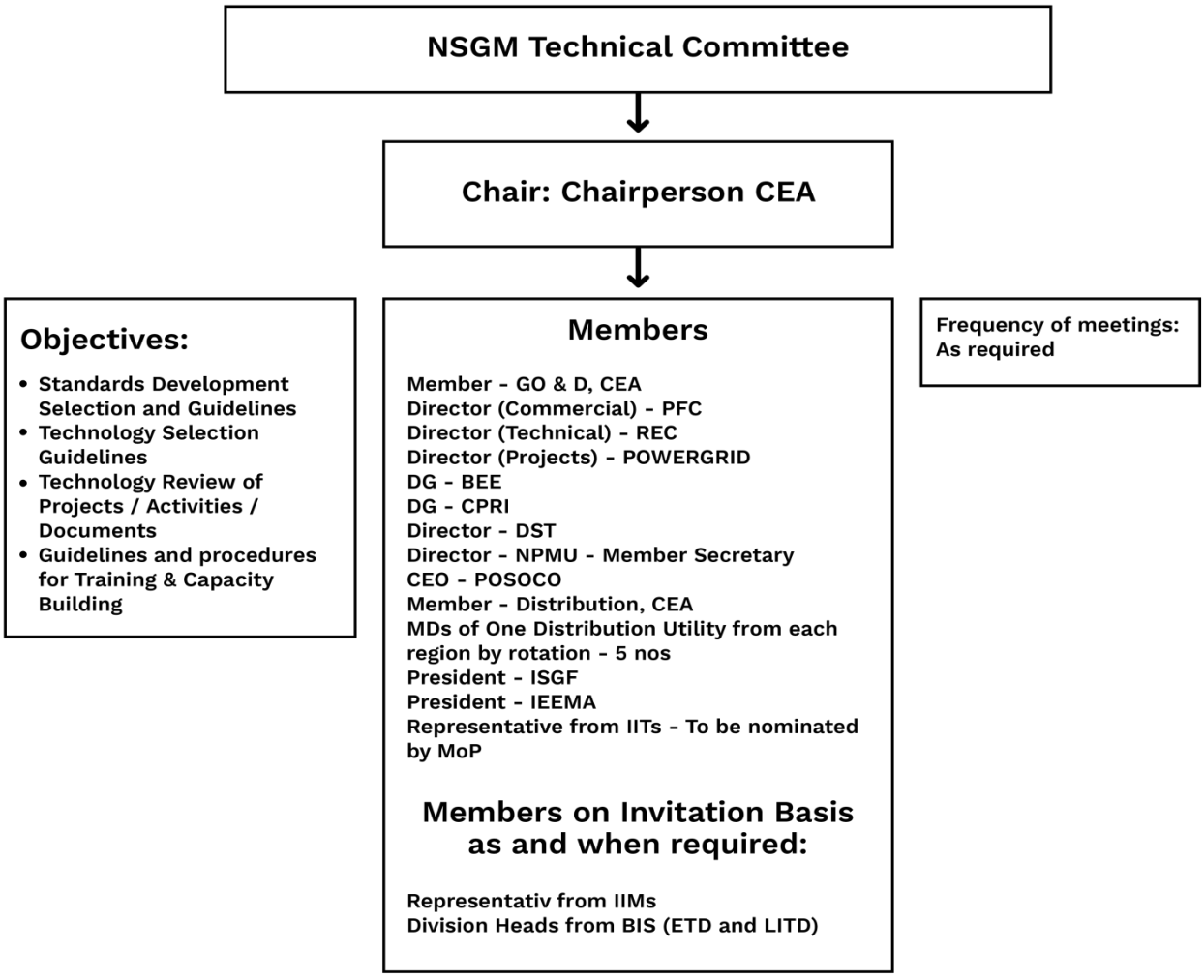
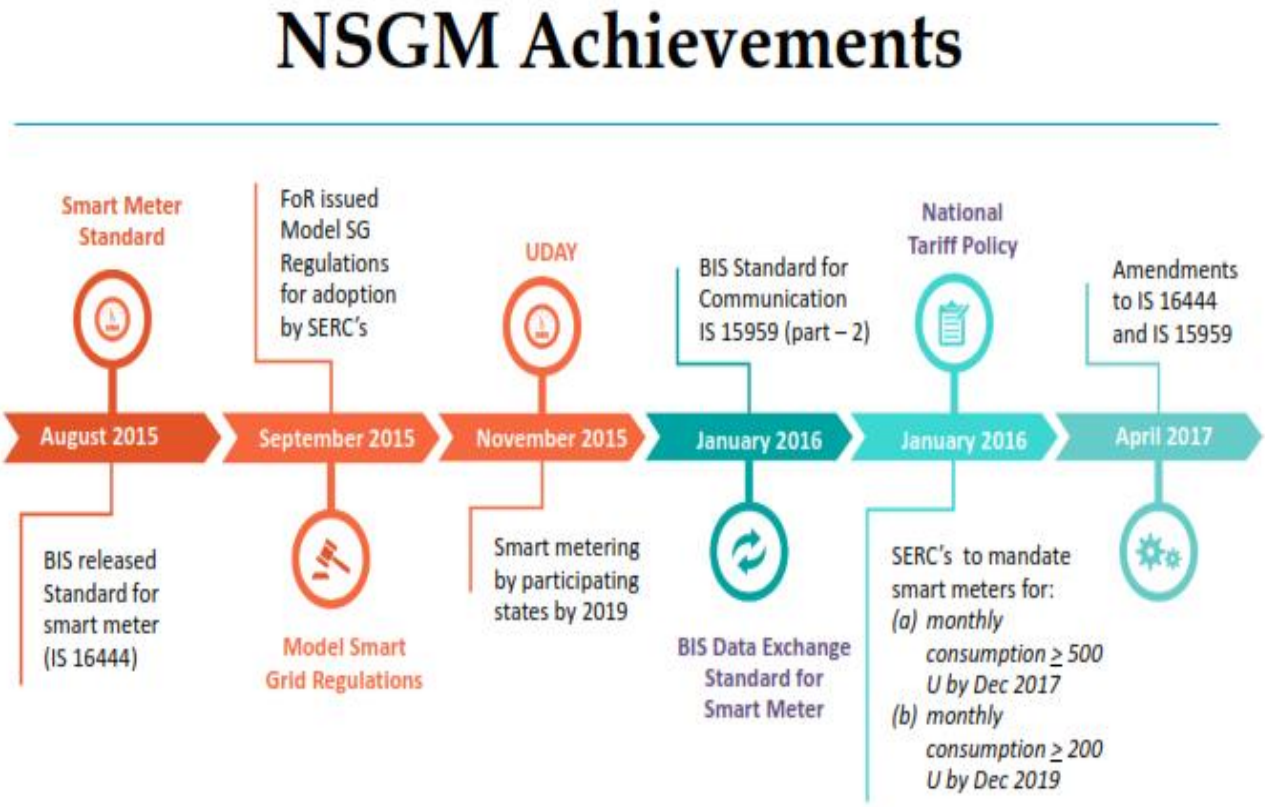

NSGM Technical Committee
Chair: Chairperson CEA
Objectives:
Standards Development Selection and Guidelines
Technology Selection Guidelines
Technology Review of Projects / Activities / Documents
Guidelines and procedures for Training & Capacity Building
Members
Member - GO & D, CEA
Director (Commercial) - PFC
Director (Technical) - REC
Director (Projects) - POWERGRID
DG - BEE
DG - CPRI
Director - DST
Director - NPMU - Member Secretary
CEO - POSOCO
Member - Distribution, CEA
MDs of One Distribution Utility from each region by rotation - 5 nos
President - ISGF
President - IEEMA
Representative from IITs - To be nominated by MoP
Members on Invitation Basis as and when required:
Representativ from IIMs
Division Heads from BIS (ETD and LITD)
Frequency of meetings: As required

FIGURE 1.5 - Tier 3

For day-to-day operations, NSGM has a NSGM Project Management Unit (NPMU) headed by the Director NPMU. Director NPMU is a Member of the Governing Council and Empowered Committee, and Member Secretary of Technical Committee. NPMU is the implementing agency for operationalizing the Smart Grid activities in the country under the guidance of Governing Council and Empowered Committee. Grant upto 30% of the project cost is available from NSGM budget. For selected components such as training & capacity building, consumer engagement etc., 100% grant is available.

1.7.2 NSGM Achievements (FIGURE 1.6)


NSGM Achievements
Smart Meter Standard
August 2015
BIS released Standard for smart meter (IS 16444)
FoR issued Model SG Regulations for adoption by SERC's
September 2015
Model Smart Grid Regulations
UDAY
November 2015
Smart metering by participating states by 2019
BIS Standard for Communication IS 15959 (part – 2)
January 2016
BIS Data Exchange Standard for Smart Meter
National Tariff Policy
January 2016
SERC's to mandate smart meters for:
(a) monthly consumption ≥ 500 U by Dec 2017
(b) monthly consumption ≥ 200 U by Dec 2019
Amendments to IS 16444 and IS 15959
April 2017

1.7.3 Regulatory Authorities in Indian Power Sector

- The Ministry of power

  Deals with planning policy formulation processing and implementation of project and treatment of legislation in regards to power generation Transmission and distribution

- Power Grid Corporation of India Limited

  Responsible for National and regional power transmission planning

- Central electricity authority

  Advises on matters related to National electricity policy and formulation of short-term and prospective plan for development of power system

- Central electricity regulatory commission and State Electricity regulatory Commission

  Regulates tariff, formulate policies regarding subsidies and promotion of efficient and environmental policies at Central and state level respectively

- Central transmission utility and state transmission utility

  Development of efficient coordinated and economical system of interstate and intrastate transmission lines.

1.8 PRIVACY INFORMATION IMPACTS ON SMART GRID

Personal or privacy information is a subject generally not associated with the utility industry. But the truth is that the utility industry has been managing customer information since its inception. The management and delivery of retail power to customers requires that the utility companies maintain a capability around this. The question is whether or not there are laws, rules, or regulations that should apply to these companies in order to protect that information. Privacy information is defined in four basic dimensions, including personal information, personal privacy, behavioral privacy, and personal communications privacy.

Personal information is defined as "aspects of an individual, or identifiers specific to an individual." As most people know, when you set up an account with an electric company, the utility company will likely require you to complete an application, similar to what you complete when you apply for a credit card. The form usually requires, at a minimum, your name, address, telephone number, and social security number. A name alone probably does not fit the description associated with the personal information description. However, combining the name with an address likely meets these criteria because of the uniqueness of the address associated with the name of the person living at the address. Moreover, utilities must collect and verify this data so that they can be sure that the person opening the account is really the person residing at the given address. Acceptance of this information almost certainly qualifies as personal information because it is meant, by definition, to denote that a person's identity is correct. The social security number can further be used to provide authentication that the data gathered clearly represents that of the applicant.

Personal privacy information is defined as the rights to control the integrity of one's body. The information collected by a utility likely does not meet these criteria because the utility likely cannot use the information to control anything regarding the integrity of the applicant's body. Personal privacy information likely does not represent information that a utility wishes to have, nor is it data that is needed.

Behavioral privacy represents the "right of individual to make their own choices about what they do and to keep certain personal behaviors from being shared with others." While information associated with an application does not alone constitute anything regarding behavioral privacy, but combined with energy usage it may. The result is that utility companies may be concerned about behavioral privacy with the implementation of Smart Grid, combined with customer energy usage data. Smart Grid at the consumer level is about trying to manipulate

users' behavior by providing them incentives to change behavior. This can be illustrated through time-of-use type programs, which likely result in a utility's ability to profile users and encourage them to change their behavior based on incentives. It should be pointed out, however, that the change in behavior is totally up to the consumer. However, if a threat were to gain access to this information, they could understand how a person uses his energy and potentially know when a consumer is at home or not. This information could of course be used by adversaries to potentially conduct crimes against the utility's customer.

Personal communications privacy refers to the "right to communicate without undue surveillance, monitoring or censorship" For this to be an issue in the Smart Grid space, utilities would have to use the information they acquire from energy usage to monitor the consumers' communications. As this is not the goal of Smart Grid efforts, it is likely that it does not represent something about which utilities should be generally concerned. Based on these dimensions, utilities have a general concern associated with privacy with regard to personal information that they knowingly collect and the potential for behavioral privacy. This is all related to what could happen if a cyber security threat were successful in stealing this information. As a result, utilities may be required to take action in an effort to prevent such data theft in order to defend themselves against any liabilities. This is mostly because they have to collect personal information in order to conduct business and will have to collect information that will lead to a breach in behavioral privacy as Smart Grid programs are implemented.

Your name, address, and telephone number are required so that the utility can catalog you as a customer and ensure that you reside within their service territory. This information may be considered personal or private, but it is relatively routine that consumers would provide this information. For example, when you acquire a telephone number, the phone company gathers this information and then publishes it in the "white pages." While you have the option to pay to have your number listed as private, the utility companies are not in the business of publishing your information. They do, however, keep this information and this is generally accepted.
Social security numbers, however, are also required and used to conduct a financial history check in order to determine the applicant's ability to make monthly payments on their utility bill. The financial history check likely includes the execution of a credit history check, which means that the utility companies must acquire one's credit score. The credit score and social security number must then be protected because they do represent personal and private information. The storage of this information means that utilities are responsible for protecting this information. This information is a likely target for attackers who wish to gather this data and then use it for potentially malicious purposes.

To deal with these potential effects, it is likely that utilities will need to execute privacy impact assessments in order to determine if they are really capturing privacy information. And if privacy information is captured, then they will have to protect it in alignment with potential laws that might apply, including but not limited to the Fourth and Fourteenth Amendments to the United States Constitution, the Privacy Act of 1974, and other laws. This of course all hinges on the likelihood that threats will break in, steal, and use this information for malicious purposes. If a social security number is stolen, for example, and this information is used to commit fraud, then the utility company would likely be found liable to the consumer for allowing the fraud to occur on their computer systems. The likely impact would be that the utility company would be required to pay for all damages associated with the theft and fraud, including payback for any money lost, restitution for the hardship faced during the loss, and, finally, identity protection for life. For one consumer, this may not be challenging, but considering that these systems may potentially store information for millions of customers, it could be extremely detrimental to the utility.

If a threat were to break into a utility that maintained a customer base of 3 million and simply steal every single social security number, what would the impact be? Considering that identity protection costs somewhere between $5 and $15 per month, taking the low cost as an example, the monetary impact to the utility losing that much information may result in a financial liability of $5 multiplied by 3 million customers. This would then represent a cost to the utility company of $15,000,000 per month every month for the life of every customer whose data was stolen. This could then represent a liability of $180,000,000 per year, which is a significant cost. As reaction to something potentially occurring, a utility might expect to employ forensics experts to come in and disprove the fact that the information was stolen or to simply try to pacify their customer base. The bottom line is that their consumers will lose trust in the company's ability to protect their information and this could potentially have a significant impact on the overall business model. It pays then for the utility company to make an investment in cyber security in order to at least prevent an event like this from occur- ring. The key will be that they would have to show that they were not negligent in storing this information and this is where cyber security comes into play.

The stronger the cyber security posture of a utility, the more it will be able to prove that it was not negligent in the storage of such information. The more it can prove this, the easier it will be for them (the utility) to shift the burden of loss back to the consumer or taxpayer. A business action that might be taken is to buy insurance and if this ever begins, we might start seeing the insurance companies to start actually regulating the utilities for the storage of privacy

information. Some action will need to be taken as systems become more interconnected through the Smart Grid in order to prevent potential loss of privacy information to malicious threat sour

1.9 SECURITY STANDARDS

Compliance has played a major role in information security over the past decade. Although there have been various organizations such as the International Standards Organization (ISO), Information Systems Audit and Control Association (ISACA), etc., none have achieved more attention than the National Institute for Standards and Technology (NIST). The E-Government Act (Public Law 107-347) passed by the 107th U.S. Congress and signed into law by the President in December 2002 recognized the importance of information security to the economic and national security interests of the United States. Title III of the E-Government Act, entitled the Federal Information Security Management Act (FISMA), requires each federal agency to develop, document, and implement an agency wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or man- aged by another agency, contractor, or other source. One of the major elements of this law included in H.R. 2458-52 states the following:

"'(3) Delegate to the agency Chief Information Officer established under section 3506 (or comparable official in an agency not covered by such section) the authority to ensure compliance with the requirements imposed on the agency under this subchapter, including—
'(A) designating a senior agency information security officer who shall
(iv) Head an office with the mission and resources to assist in ensuring agency compliance with this section;' and
'(B) Developing and maintaining an agency wide information security program as required by subsection (b).'"

Additionally, under § 3544 identified Federal Agency Responsibilities, which include the fact that they are required to develop and implement an agency wide information security plan to provide information security for the operations and assets of the agency. The head of each agency is responsible for adequately ensuring the confidentiality, integrity, and availability of information and information systems supporting the agency operations and assets; developing and implementing information security policies, procedures, and control techniques sufficient to afford security protections commensurate with the risk and magnitude of the harm resulting from unauthorized disclosure, disruption, modification, or destruction of information collected or maintained by or for the agency; and ensuring that the agency's information security plan is practiced throughout the life cycle of each agency system.

The FISMA Act of 2002 was really the first major attempt to establish the field of information security formally outside the Department of Defense (DOD) and the National Security Agency (NSA). The DOD and NSA have maintained strong cyber security programs for some time, as a result of their line of business. Virtual attacks on computer information systems are generally nothing new. The DOD, for example, is involved in warfare and information security was likely implemented long ago in order to protect their classified and confidential information from their adversaries. The same is true for the NSA and likely the Department of Energy (DOE). The introduction of FISMA basically extended those practices into the non-DOD/NSA/DOE agencies. For example, the U.S. Department of Interior (DOI), Department of Agriculture, etc. were now required to establish formal information security programs. As the need for these programs gained traction through Inspector General assessments, etc., more of these agencies began to turn to the U.S. Department of Commerce's NIST organization.

NIST Special Publication 800-26 was an attempt to get organizations to conduct evaluations of cyber security posture and to establish their level of maturity based on what was found. This was an attempt to quantify information security risks and measure the effectiveness of the organization. While this approach represented a solid approach to identifying potential weaknesses, it did not provide a roadmap for how risk could be mitigated should weaknesses be identified. NIST later came up with SP 800-53, which represented a controls-based approach to identifying risk. The SP 800-53 approach was also one of the first standards defined to be cyber security standards. The U.S. Department of Energy Power Marketing Administrations (PMAs) are federal transmission organizations with multiple control center systems throughout the United States.

The Bonneville, Western, and Southwestern Power Administrations represent utility companies that are federally owned and conduct energy management on a massive scale. Because they are federal agencies, they are required to meet the NIST-based approach to information security. This means that they had to define their FISMA systems in alignment with the Title III of the E-Government Act of 2002. The results were that their control center systems are considered "FISMA Systems" and were thus subject to the controls defined in NIST SP 800-53. Meanwhile, FERC issued Order 706, which required the development and implementation of the NERC CIP Standards, for application to North American utility companies. As the PMA federal agencies are also utilities bound to the oversight of NERC, they were required to also meet the NERC CIP standards, in addition to NIST SP 800-53 at the same time. This was also true for other federal entities that provided power operations and generation support for the general public such as the Bureau of Reclamation and Army Corp of Engineers who many times

own and operate the major dams throughout the United States. This may have, in effect, been the genesis of where the need for greater Smart Grid security standards actually began. The PMAs, BOR (Bureau of Reclamation), and the Army Corp of Engineers are unique in this light because federal oversight is conducted by the Inspector General, who has responsibility for oversight of their control center systems with regard to cyber security posture. At the same time, NERC was prepared to regulate those same control center systems with its CIP standards. When analyzing the impact of implementation between the two sets of standards, it becomes inherently obvious that one set understands the concept of reliability while the other pushes cyber security in a manner that is a risk to reliability.

The NERC CIP standards are process oriented, as they emphasize the need for procedures versus the actual implementation of security controls on the assets themselves. Although they bring the concepts of cyber security to the control center environment, they do it in a manner that will have the least impact on reliability. The concept of asset management according to NERC CIP is to figure out what the most critical cyber- assets are that are needed to manage bulk energy and effectively exclude all others from regulation. Once the cyber-assets that need to be protected are identified, NERC CIP focuses on the need to develop an access control program capability in order to manage access to the environments where they reside in addition to other security control processes and procedures. This is done through multiple standards within the NERC CIP framework in order to control physical access, electronic access, access to electronic and physical information, as well as access to badge readers and firewalls.

The standards are unique because they require the development of a process to ensure that personnel with any of these access types complete a background investigation and have cyber security training related to their organizational role, and that all specific access types, including records, be maintained and available for audits. Because the audits are measured, utilities are forced into a situation where they must clearly manage and maintain these records, resulting in the creation of effective processes. Security controls on assets are addressed on a limited scale, where the standard requires the implementation of patches, anti- virus, log monitoring, account management, vulnerability assessments, procedures to test cyber security posture when changes are made, as well as the need to dispose of assets properly prior to removal. And finally, disaster recovery and incident response processes must be developed, implemented, and tested in order to meet the standards.

NERC also out- lines a process for taking exceptions to the standards, which are executed whenever the utility comes across a system that cannot implement the security controls that

have been prescribed. The benefit of implementing these standards in this fashion is that it is really left up to the utility on how to do something, and it is known that whatever they decide to do, it must produce the records required for an audit and these records are measurable. The downside becomes however that overall cyber security risk is not really addressed as the utilities instead focus on complying rather than understanding the threat.

NIST takes on a different approach to securing the architecture. The E-Government Act of 2002 requires that whole architectures be identified fully, and that all security controls and the concept of risk management be applied to those architectures. Furthermore, the list of NIST SP 800-53 controls is much more detailed and much more expansive. For example, there are eighteen control families, with multiple controls spread out through each family, all segmented by the concept of impact that has been established for the architecture in alignment with NIST SP 800-60, "Guide for Mapping Types of Information and Information Systems to Security Categories." The approach requires that all your systems be identified and each one quantified for impact. Based on impact, you are required to apply controls defined in NIST SP 800-53 using the high, medium, and low concept as represented in the impact study. Furthermore, there is no process for taking exceptions, only the ability to identify and accept risk. NIST SP 800-53 emphasizes risk management while NERC CIP focuses on compliance. Both are intended to elicit security: one achieves that through the identification of risk and its acceptance with a broad scope, while the other achieves success through scope limitation and the requirement to achieve specific measurable objectives, including reports and audit trails that prove implementation. Table 1.2 illustrates the key differences between the two concepts.

Although it is not certain how NIST came to focus on energy management systems, it is clear that the PMAs, BOR, and the Army Corps of Engineers had some influence on this because of the need to satisfy both NIST and NERC. Needless to say, NIST began to include security controls focused on transmission organizations into their 800-53 standards. This was done even while NIST understood that NERC CIP was the regulatory authority over transmission control systems. NERC has since begun the development of version 4 of its standards.

This version proposes an impact based concept that should include the full scope of energy management. The concept of energy management represents multiple facets within a utility company. These facets are usually represented as Generation, Transmission, Distribution, and Metering. Each of these facets plays a role in the management of energy throughout the United States and various utilities play different roles in each. Furthermore, NERC, understanding that a more comprehensive solution for securing cyber assets is coming, is proposing to allow for

other cyber security frameworks such as ISO, NIST, COBIT (Control Objectives for Information and related Technology), etc. to be used to manage cyber security. While these frameworks may not be effective in the manage- ment of control system security, the flexibility is meant to lead organizations to draw their own conclusions or potentially develop a more robust energy sector framework.

NIST SP 800-53	NERC CIP
All systems are defined	Systems defined by function
Criticality used to identify impact level	Critical Impact is the only level identified
Risk Management approach	Compliance-based approach
Confidentiality, Integrity, Availability	Reliability

Table 1.2 NIST versus NERC.

This leads us to today, where NIST has drafted NISTIR 7628, "Smart Grid Cyber Security Strategy and Requirements." This document is the latest in a line of planning elements that were initiated in order to develop a strategy for securing both energy management and Smart Grid systems. The term "Smart Grid" is more and more becoming the terminology of choice when identifying energy management systems, whether they are in metering, distribution, generation, or transmission systems. The point is that appropriate planning is going on to develop a more comprehensive solution that takes the best parts of NIST SP 800-53 and aligns them with the concept of reliability and the objectives that NERC wishes to achieve.

1.10 SMART GRID SECURITY STRATEGY

Vulnerabilities are identified based on gaps in the required security controls. That is, you need to know which security controls are needed in order to identify risks using internal and external threats as tools that threaten the system in question. There are security controls that prevent external threats from breaking into a system and controls to augment security associated with internal threats. In both cases, there is always the threat that someone or something will attempt to access your environment, compromise your systems, and create a liability for your organization. The liability to the organization represents the impact in the risk equation probability x impact = risk. To measure risk, you need to understand the impact and what the likelihood is that the impact will be realized. This is an important concept to grasp when it

comes to the world of Smart Grid because the traditional boundaries that segmented external from internal threats are no longer relevant. Furthermore, the impacts that can be realized in Smart Grid extend beyond the world of identity theft and into the realm of risk to human life and even humanity itself.

Threats are generally constant because they threaten the organization's ability to secure itself against risks that have been identified. The difference between an external and an internal threat has to do with the concept of cyber-risk versus cyber security risk. A cyber-risk is defined as a risk that threatens the reliability of a cyber-asset within a Smart Grid architecture. This includes the potential that a staff member may improperly operate a Smart Grid system, resulting in an undesired impact. An example could be an employee tripping over a power cord in the data center and causing a server that supports Smart Grid tech- nology to stop working.

This is a cyber risk because it is not a risk as a result of a malicious threat, while a cyber security risk should be associated with a malicious event that threatens to cause the same impact or liability to the organization. For example, if an employee intentionally tripped over a power cord, then this is a cyber security risk because that person intentionally tried to cause harm to the stability of the system. The two concepts are important to understand because of the way that utilities view risk to their energy management platforms. The goal of the cyber security professional should be to identify whether or not a cyber-risk is actually a cyber security risk. And this is the problem represented when discussing how to secure Smart Grid technology.

A malicious external threat source has the intention of creating the same cyber-risks that utilities are concerned about; however, the view from the utilities is that cyber security threats are somehow different from cyber threats. This difference has to do with external versus internal threat. In other words, utilities are concerned with internal threats and are happy to implement controls to prevent them, because there is a long history of them causing outages and events that impact the reliability of their energy management systems. Whereas, external threats represent traditional hacker-type risks because there is a limited history of them impacting their energy management systems.

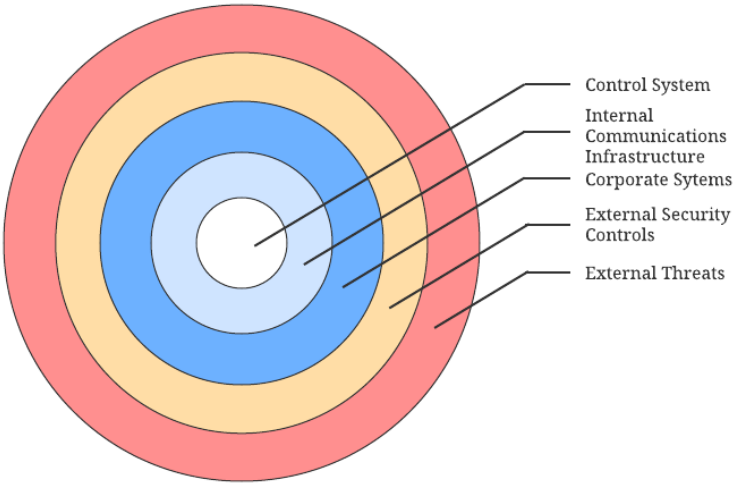


FIGURE 1.7 Control system location

Whether it's internal cyber risk or external cyber security risk, controls must be implemented to mitigate both risks types. The general method of securing against these threats is to implement technical controls, usually network based, that prevent external threats from accessing or even seeing the energy management system, for example. Most utilities have isolated their control systems, which end up being networks buried deep in their corporate networks. There are almost always firewalls between networks; that is where the air gapped view derives.

The risk that is quickly becoming an issue is where these access control points are opened so that the operational users can access their equipment more easily. Going back to the example of remote access to relays, it will be much easier to have all the technicians essentially sit at their desks and control them from their corporate desktops. From a reliability perspective, this is good because the quicker they can get to them, the faster problems can be solved. However, from a cyber security perspective, even with the use of VPNs, point-to-point firewall rules, etc., the door is opening from the corporate network into the operations network. This implies that the air gap will slowly go away over time and threats may start to find their way into the control systems. Figure 1.7 illustrates where the control systems reside in relation to the common network configuration.

External threats generally threaten the external security of the organization. As the control system is protected at the core of the organization, it are perceived as not vulnerable (despite vulnerabilities that exist in their systems) to external threats. Keep in mind what was stated earlier, that traditional IT security controls many times cannot be applied to these assets, so if they were ever exposed to traditional IT threats such as malware, it would not take much to knock them over. Moreover, there is merit associated with this utility belief because there have

not been any or many reported penetrations of networks all the way into the control system that have resulted in the big impacts with which utilities are concerned. Instead, utilities are more concerned with internal threats, of which there is a lot of evidence that demonstrates that large impacts have been realized as a result of cyber risk. These risks are generally associated with operator error or conditions in which a control was used that should not have been used based on a miscalculated condition.

Internal threats are secured against using process control, hence "process control system." Control systems are effectively just processes that are used to control other processes. So the natural method of securing process control systems is through process control itself. This is why the NERC CIP standards are written from a process-oriented perspective. One should track and manage users who have access to the environment so that they know that access is privileged, and they understand what their responsibilities are associated with such access. This does not mean that access is restricted for users; it just means that their access is known and hopefully the risk of such access will be identified at some point in the future.

Whereas, the NIST-based approach takes into account the risk and is looking for more of a role-based access control solution. This is not to say that NIST does not take this into account; it simply illustrates the point that NIST views the problem differently from NERC. Remember that NERC is really about allowing everybody to continue what they are doing so that reliability is not impacted, but the utility should just know who has access. NIST is more about looking at who has access and trying to figure out whether or not they really need it. Both standards have their flaws, NERC from a cyber security risk perspective and NIST from a reliability perspective.

The reason that utilities prefers the NERC approach is that they believe and trust in their trained engineers and they know that their number one priority is reliability, so they need to be able to do whatever they need to do to make the system work. If an engineer ever gets into a situation where she cannot do something that she needs to do because she was viewed as not needing the access to be able to ever do it, we could potentially see a power out- age that was caused because access was restricted that is the fear. Keep in mind that these are real-time systems, and reaction to normal events may only allow for a response to occur in seconds; if that response does not occur, then outages and problems become possible.

Req. ID	Control Name	Gap Description
AC-1	Access Control Policy and Procedures	No policy exists which requires that access controls be in place.
AC-2	Account Management	There is no common process for managing user accounts for assets within the architecture.
AC- 3	Access Enforcement	There is no mechanism which enforces access controls to and from assets within the architecture.
AC-4	Information Flow Enforcement	There is no mechanism to control the flow of information to and from assets within the architecture.
AC-5	Separation of Duties	Role-based access control is not implemented for assets within the architecture.

Table 1.4 Security control gaps.

The way this should probably be approached is that controls should be categorized based on impact to the control system, and more flexibility should be allowed where those controls have a higher propensity to cause reliability concerns. At the same time, the capability to react to security through monitoring needs to advance to a point where it can be used to prevent and respond to cyber security-related events. For example, if an engineer does something that is out of the ordinary, and his action is malicious, then cyber security should understand what that is and how to react to it. The risk of preventing something is probably greater than the risk of a cyber security event happening, so a reactive approach will likely be the best option. Weighting of controls based on the mission of the organization then must be taken into account in order to integrate cyber security standards that will be viewed as actually augmenting security posture.

The point is that when evaluating risk to a Smart Grid architecture, one needs to understand that there will always be risk based on internal and external threats. Second, a security controls approach should be used to identify gaps so that they can be analyzed for risk. Using the NIST SP 800-53 set of security access security controls, if architecture has gaps associated with each of the controls represented in the following figure, then what are the risks? See Table 1.4.

The risks associated with these gaps must be identified in the context of external and internal threats. Given the gap, what weakness is present, and can that weakness be exploited by an internal or external threat? Table 1.5 breaks down each gap according to the threats identified. In this case, a business case has been made for implementing a control to mitigate the risk of either an internal or external threat.

The business case is made by illustrating the risks associated with the lack of security controls illustrated. If the organization, for example, does not have an access control policy, then why would administrators implement access control? And if administrators do not implement access control, then what will prevent internal users with no need for access to critical resources from accessing critical resources? A policy will be very effective in preventing a non malicious act by a user because the user would be aware of something he is not supposed to do, but at the same time not actually restricted from doing what he needs to do in order to react to something that needs to be done. This would even be effective where the security control cannot be implemented to prevent access. The external threat, however, is not going to care about the policy as it is written and with no access controls in place will simply access the resources that he knows he is not supposed to access. Based on the example above, we know what the risk is and we know that the implementation of the control will prevent the risk to some extent. However, what happens if the control cannot be implemented because the control itself represents a risk?

As is the case in Smart Grid architectures, security controls themselves represent liabilities, more so to control systems. Using the example from Table 1.4, it is obvious that policy can be implemented, but a technical solution to actually restrict access may not be possible because it represents another hop for the assets and thus could result in bad performance. As bad performance is counter to the support of reliability, such a control may represent a cyber-risk to the architecture itself. So if the control represents a risk and lack of the control represents a risk, then how is risk mitigated? The answer is through the identification of an alternative control. This will more than likely be a process control that places a restriction on behavior so that a technical control can be implemented to detect anomalies in behavior. Again referring back to our list of gaps, where controls cannot be implemented, what alternative controls can be used to mitigate the risks identified? Table 1.6 illustrates this.

The key to securing Smart Grid architectures using risk based techniques is then to identify the mitigation strategy for a risk that exists because a security control is not present and associate it with what an internal resource might end up doing and the impact that would be caused as a

result. Identifying the cyber-risk is likely more important than the cyber security risks because they are more likely to occur. Moreover, utilities will pay more attention to cyber-risk because they understand that the chance of occurrence remains high without mitigation because accidents have occurred in the past. What should be noted, however, is that if an external threat were to gain access to internal resources that threat would attempt to maliciously cause accidents to occur that would ordinarily be caused by an internal threat. Understanding this concept will help utilities and security professionals understand that the reality is that there is no difference between an impact that can be caused by an internal or external threat.

Therefore, the security controls should be implemented in order to prevent both threats from being able to successfully create an unwanted impact. Moreover, cyber security professionals are going to be able to mitigate far more risk from the perspective of an internal threat than they will by simply focusing on an external threat. And they will, at the same time, be preventing an external threat from exploiting internal weaknesses should access control barriers ever break down.

Control Name	Internal Threat	External Threat
Access Control Policy and Procedures	Without access control policies and procedures users may access systems for which they are not supposed to and are not trained to use, resulting in the potential that the systems may be used in an unauthorized manner.	Lack of an access control policy and procedure may lead to not properly implementing controls which prevent external threats from accessing internal resources.
Account Management	Without account management there is no way to differentiate between users who are supposed to access systems and those who are not.	Lack of account management may make it easier for an external threat to escalate privileges on user accounts if they have penetrated the architecture.
Access Enforcement	Without access enforcement there is no way to restrict access to systems by users who should not have access.	Lack of access enforcement may allow for an external threat to access the architecture from the outside because access

		restrictions may not be implemented.
Information Flow Enforcement	Without information flow enforcement there is no way to control what users do with information from systems within the architecture.	Lack of information flow enforcement may lead to an external threat gaining insider information about the makeup of the target architecture.
Separation of Duties	Without roles-based access controls there will be no way to identify who caused a cyber-risk in the event that one occurs because all users will have equal access despite their access needs.	Lack of separation of duties may allow for an external threat which has compromised a user account to access any resource inside that they desire.

Table 1.5 Threat assessments.

Control Name	**Process Mitigation**	**Technical Mitigation**	**Threat Mitigation**
Access Control Policy and Procedures	Develop and implement an Access Control Policy and Procedures for provisioning access.	Centralize management of access control policies, so that users are forced to engage an authority to be provided with access.	Internal Threat contained by process mitigation. External Threat contained by technical mitigation.
Account Management	Implement an account provisioning process.	Centralized account management solution that reports changes to user accounts.	Internal Threat contained by process mitigation. External Threat contained by technical mitigation.
Access Enforcement	Require all access be default deny and require a change control process to open needed access.	Reports of changes to access controls.	Internal Threat contained by process mitigation. External Threat contained by technical

			mitigation.
Information Flow Enforcement	Implement an information characterization and classification process.	Data loss and prevention solution.	Internal Threat contained by process mitigation. External Threat contained by technical mitigation.
Separation of Duties	Develop roles and associate users to role types	Implement roles-based access controls associated with account management.	Internal Threat contained by process mitigation. External Threat contained by technical mitigation.

Table 1.6 Risk Mitigation.

1.11 **SMART GRID IMPACTS**

NERC CIP 002 Critical Asset Identification illustrates a methodology for identifying assets that are critical to the bulk electric system. This methodology, however, does not truly address all aspects of utility assets,including distribution, advanced metering, and some generation assets. This is an important notation because assets that make up Smart Grid must be evaluated for impact before we can understand the risks associated with the cyber-assets within them. The current NERC CIP methodology takes into account assets that meet the following conditions:

- Control centers and backup control centers
- Special protection schemes
- Automatic load shedding
- Generation resources critical to the reliability of the bulk electric system
- Transmission resources critical to the reliability of the bulk electric system
- Assets critical to system restoration

The most recent version of this methodology, known as CIP 002 version 4, further defines how these criteria end up being critical by applying the bright line concept. This bright line concept is only applicable to the transmission and generation resource requirements, providing clear guidance on what is and what is not critical. For example, generation facilities that have a total output of less than 1,500 megawatts are not considered “critical assets.” This methodology has

been established to address the criticality of assets for the bulk electric system. While this is important, it is equally important to understand the impact for the other areas of Smart Grid because risk cannot truly be quantified until impact has been determined.

NIST SP 800-60, "Guide for Mapping Types of Information and Information Systems to Security Categories," perhaps provides a frame- work for evaluating the criticality of assets within Smart Grid. While the methodology does not necessarily apply to Smart Grid, it can potentially be modified to further provide a way to measure impact for Smart Grid assets. The point is that a library of impacts for each component of Smart Grid must be developed so that it can be used to evaluate the risk to confidentiality, integrity, and availability. This can be accomplished when viewing each component within Smart Grid by asking simple questions in relation to confidentiality, integrity, and availability.

Figure 1.7 illustrates a method for simplistically identifying impact. Security Area references the standard confidentiality, integrity, and availability associated with the impact type. Confidentiality refers to the impact of disclosure of something associated with the asset type. The loss of information associated with the asset, for example, and whether or not the impact of such an event is high, medium, or low based on the view of the organization. Integrity refers to a loss of integrity, which is more closely associated with the concern that the asset may be controlled by an unauthorized party. And Availability deals with the concern if the system were made to be unavailable.

An example of how the table in Table 1.7 might be used to determine impact on a Smart Grid asset would include an analysis of this information associated with the asset. If, for example, we were talking about a smart meter communications infrastructure, how would these questions be answered? What is the impact if the system (asset) were to be hijacked by an unauthorized party? The reviewer would ask questions along these lines to view part of the impact of having an integrity breach in the context of cyber security. What could an attacker do, for instance, if she were able to hijack the communications infrastructure for a smart metering deployment?

One answer might be that she would be able to monitor all communications and potentially Redirect where that information goes to. The result could be that the utility that owns the deployment may not get the data it needs to effectively bill the customer. And the question to the utility should be: how would this affect our business? The utility will most likely be concerned with the likelihood that some- thing like this could occur and should it, the impact would likely be high for a number of reasons.

Security Area	Impact Description	Impact Discriminator	Impact Risk
Confidentiality	Loss of Information	What is the impact to the system if information is lost or stolen?	High, Medium, or Low
Integrity	Loss of Control Loss of Data Integrity	What is the impact to the system if it is hijacked by an unauthorized party?	High, Medium, or Low
		What is the impact if the system provides invalid data?	High, Medium, or Low
Availability	Short-Term Denial of Service Long-Term Denial of Service	What is the impact if the system is down for less than 48 hours?	High, Medium, or Low
		What is the impact if the system is down for more than 48 hours?	High, Medium, or Low

Table. 1.7 Simple impact table.

It is important to understand those reasons, which can later be used to demonstrate why a certain control should or should not be implemented.

Impact goes hand in hand with the application of security controls. This is because the lack of controls leads to a heightened probability that the unwanted event can occur. There are various models for impact Categorization as discussed above, and those should be used to improve the ability to identify impact. The key is going to be making it as simple as possible so that the

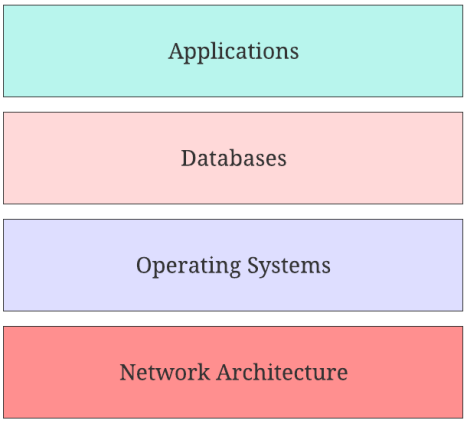


FIGURE 1.8 IT-enabling asset types.

organization can easily recognize that something can happen and that mitigation of the impact should be of primary concern. Creating a list of impacts associated with different scenarios also allows for the identification of security project tasks that can be used to mitigate the risk. Trying of that control will be accepted, these directly back to a control standard will likely justify why it is being implemented. The more that a security control can mitigate an impact on one or more assets, the more likely it is that the implementation

1.12 APPLYING SECURITY CONTROL FRAMEWORKS TO SMART GRID

There are four common sets of assets regardless of architecture type: applications, databases, operating platforms, and network devices. Smart Grid is no different; however, it is perceived to be because embedded versions of operating systems are used or industrial control systems that function based on logic are used. Regardless of this, they still represent the four basic forms of information technology enabling assets (Figure 1.8).

Industrial control components, meters, and other devices that make up Smart Grid but are not applications, databases, operating systems, or network architecture are at least a hybrid of several or rely on control from an application. In each of these cases, these things must be secured independently of process in order to mitigate risk to the components.

There are a few basic problems with today's risk management models, in the context of 800-53. NIST SP 800-39 provides guidance on risk management but assumes that you have the resources to properly execute and acquire all that information. NIST SP 800-53 maintains more than 500 controls that depend on how the system being analyzed is classified. Furthermore, it does not really take into account the specific components of the system being analyzed. And then there is the question of what constitutes a system or a network. Defining system literally in broad terms is probably the most accepted method and then to categorize assets based on what they are used for in supporting the system. For example, a Web portal may be considered a "system," whereas the Apache Web server, Linux operating platform supporting Apache, the Oracle database that the Apache Web server connects to, and the Microsoft Windows server that supports the database should all be considered assets.

The web server application is an asset because security controls can be implemented on it, for the same reason that the database and operating systems should be considered assets. One might even consider the network components that manage connectivity for these assets to be assets within thesame system themselves. The general view of such an architecture appears in Figure 1.9.

The "system" in this case would be the entire architecture illustrated. The assets involved are less obvious; the web server is really two assets, while the switch and the firewall represent two assets and the database server and associated operating system represent two assets. In total there are six assets, all of which have different security settings. From a risk management perspective, the question is whether or not you want to have a switch brokering access to your database server, which has limited security capability implemented, or do you, for example, want to restrict what is allowed to communicate with that database server at the switch and firewall? Then there is the larger question of how all of this will be managed.

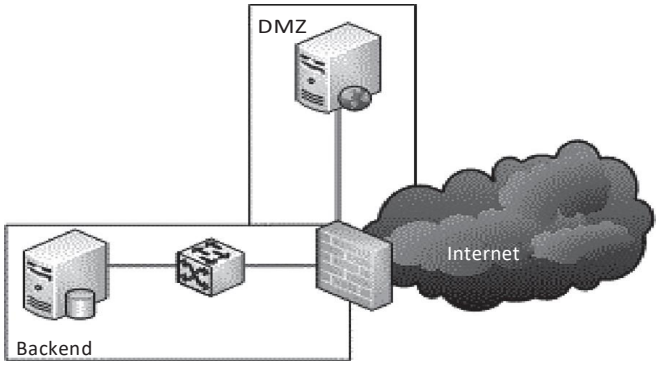


FIGURE 1.9 Example generic network architecture.

NIST provides guidance on how to conduct the system assessment for Technical, Operation, and Management Controls; the problem is that most people conducting such an assessment really won't understand that access control applies to all six assets in this case. You can develop policies that mandate that these systems meet certain criteria, or you can start from the bottom and try to harden all the assets. The trouble is that you never truly accomplish your goal, and it is still difficult to measure risk in this instance.

There are numerous combinations that you can use to determine what the risks are, but quantitatively it is difficult if not impossible to do. And then when you begin thinking about how many assets there are and how many systems an entity might have, it is difficult to imagine running through the full NIST SP 800-53 control catalog for every system; especially considering the costs, does it really outweigh the benefit? In either case, the goal is to understand which security controls are implemented from an operational management perspective for the overall system and what the technical security posture of each individual asset is.

Assessing each asset independently using the technical controls from within the technical controls family is probably the quickest method for building a unique asset security profile. You can ask simple questions such as does the web server require all users (administrators and end users) to identify themselves? If the answer is yes, then the next question relates to what kind of authentication is required and what is the extent of that authentication. If the answer ultimately ends up being that all six of my assets require unique identification, and they all require eight character passwords for use and token based authentication for administration, then I know that my asset risk is relatively low in terms of this control. If I, however, do not have any logging mechanism set up and I do not lock out accounts after unsuccessful log-on attempts, never apply patches, etc., then that asset risk increases significantly. This is why there are certain questions that you want to know of for each unique asset type in terms of configuration.

At the same time, you want to make sure that the organization has an operational plan for implementing operational controls across multiple "systems." These controls only represent that the entity wants certain controls implemented, but do not illustrate whether or not this is actually true. For example, I might write a plan on how I am going to control change in my environment, aligning with the NIST SP 800- 53 Configuration Management family; but even with this policy implemented, there is no assurance that all of my assets follow it. Assuming I was not following the policy written, but the policy or plan was written to the exact specifications of NIST, I might end up with low risk in regard to what security management

desires and high risk with what is actually implemented. The question becomes: Which risk has more weight, and how would the two be combined? And there is even a larger problem in determining the probability of occurrence because there really is no way to illustrate how threat sources might exploit your lack of controls. In other words, there are a lot of factors to consider when measuring risk in regard to information security.

Perfection in information security is generally not possible, because everything depends on something else. This is true for risk management; if I call something a high risk, and then there are likely a number of reasons why it is not a high risk. To quantify, this will require a lot of work and, in reality, I am just wasting a lot of time trying to prove that something is or is not true. The reality of the situation is that the head of any organization wants to know what the risk of an information security problem is for the entire network. Whereas, their subordinates may want to know what the risk is for each function and their subordinates of the risks to the systems and so on. Based on this information, the concept of identifying weaknesses in the organization's security posture should likely be applied at the general level. So, if I have no patch management plan, patch all my windows servers, and sometimes patch my UNIX servers in the same "system," I might say that my system integrity risk is moderate high. This is mostly because there is no management commitment to patch management and only one of the two unique systems types in the environment is doing what is required.

The most feasible solution is to broadly look at the controls catalog for each unique asset type and then determine what the risk level is for operational management of that environment. Table1.10 illustrates an example of the results needed to begin illustrating risk, using the content described above.

This approach allows you to visualize where assets are in terms of security controls and demonstrate how compensating controls can be used to protect assets that do not maintain the proper controls. For example, the firewall maintains the ability to restrict access to itself and other systems. However, the network switch may not maintain this capability. If the firewall is connected to the switch, then you are able to specifically control who is able to directly access the switch. This concept is known as controls inheritance and is important to understand, especially in environments where controls cannot be implemented.

The basic premise here is that now reds can be turned to yellow based on the ability to inherit controls. The following bullet list demonstrates how this control inheritance would be implemented using the assessment results from above:

- Apache Web server inherits access control and audit/account ability from the Linux operating system.
- Apache Web server inherits access control and audit/account- ability from the firewall.
- Network switch inherits access control and audit/accountability from the firewall.
- Oracle database inherits access control, identification, and audit/accountability from the Microsoft operating system.

Operational Assessment			
Control	Description	Results	Risk
System Integrity Protections	Are patch management processes available for all platforms and applications within the environment?	No	
Configuration Management	Is there a plan to baseline the security configuration for each asset?	No	
Contingency Planning	Has a plan been developed to restore the system in the event of failure?	No	
Incident Management	Is there an incident management plan for the environment?	No	

Table 1.10 Security assessments.

The controls inherited by each asset with gaps demonstrate that each asset type is still protected even though it cannot or does not meet the standard on its own. Looking at the example provided, one notices that there are inconsistent security configurations on the assets within the architecture. This is most likely because there is no plan for base lining the configuration of each unique asset type as seen in the "Operational Assessment." Furthermore, in this example environment, no plans have been developed to augment security, which is likely why there are inconsistent controls being applied. For example, the network switch has the capability to do access control, but it is not implemented because the team managing the device may not be required to turn on that feature.

This is generally where you find vulnerabilities in most enterprises, because there are inconsistent controls applied and that means that gaps can exist. Threat sources (hackers or other malicious users) are generally looking for a breakdown in security that can be exploited. More advanced threats look for weaknesses in the vendor-created products, which is a separate risk that the organization cannot really control.

The controls inheritance process demonstrates that the system is really protected, but the lack of planning may demonstrate that in the changing future, this may not be the case. For example, if no plan exists for base lining the security configuration of assets before being placed into service, it may be possible that an asset replacement being done under new management will not be secured as the old one was. This is because the previous manager took security seriously and verbally required that all assets be configured securely before being placed into production. But the new manager may be more concerned about getting things done quickly and decide to not require secure configurations, thus opening the door to risk. However, if a plan or process were developed that was universally mandated, then it would not matter who the manager was, as there would be something for reference and following the plan would likely be implied.

Risk management is a concept that needs to be ongoing and used to thoroughly evaluate cyber and cyber security risk in order to identify weaknesses and their planned remediation. To properly understand likelihood, we need to understand the risks associated with the individual cyber-assets. We then need to pair that risk with the overall impact identified with each of the assets where the individual cyber assets are located.

1.13 MANAGING THE OVERALL RISK TO SMART GRID

Understanding the utilities and how they relate to one another including the relationships with vendors and the government at the federal, state and local levels is key to a good risk management strategy. Utilities as most companies, are typically vertically oriented, as they maintain business areas that support the various areas of grid management. Understanding these verticals and why they exist will allow for the development of a risk management strategy. Verticals within a utility are defined generally to serve a specific function. For example, there are organizations within grid operations that support the various elements of the grid. Substations are usually managed by a group that is separate from the group that maintains the control center. And power generation groups are usually independent of substation and control center groups, as well as autonomous amongst themselves. Finally smart meter groups are different from all three of the others, as they are focused on power delivery and billing at the consumer level. The separation of duties between these groups and the power plants contributes to the complexity in understanding the cyber risk associated with each. This is because each group views the power grid differently.

From the substation group's perspective, the concern is generally in the maintenance and well being of assets distributed across a wide geographical plain. Substations can be anywhere and because of this, they are many times unmanned. Meaning that there are many substations which do not have people working in them on a regular basis. This is due in part to the physical

location of these assets, as they can reside in locations which may be considered inhospitable for human inhabit- ant. And these substations will maintain field systems, which are used to manage and maintain assets within the switchyard that the substation is meant to support. From the perspective of this group, maintenance and communications are of extreme importance. If the field systems are not properly maintained and fail, it may take a considerable amount of time to restore or replace them, because of the location of the assets themselves.

As a result, maintenance crews and periodic visits to check the current state and conditions of these facilities are required. Communications is of extreme importance to these facilities as well, because it is the only way that they can enable remote support of the field systems assets. Furthermore remote connectivity to these sites is necessary for other business areas within grid operations, so that the necessary monitoring and control capabilities can be used to support overall grid health. The mission of the substation group is then much different from the mission of the control center, generation or metering side of the organization.

The control center group functions in two capacities, one to actually conduct command and control, why the other serves to support the systems that are used to provide this initial function. The team that sup- ports command and control is tasked with actually utilizing the applications and systems needed to support grid operations. They are highly trained engineers and technicians, who understand how the big picture grid functions and how to read the various monitoring tools implemented to provide the current status of grid assets. A fault on a line for example, might be viewed from a control center terminal. The response to such a fault might be for an operator to isolate it and then notify a line crew to physically visit the location and correct the problem. This makes the applications that are used for such monitoring critical and those applications are managed by a separate team that is IT centric, typically referred to as the SCADA group.

The SCADA group is really just an IT organization with specialization in the realm of real-time systems. The specialization extends from the fact that they understand how the applications work and can provide immediate support in the event that one of these critical applications fails. The specialization is important because of the criticality involved in having the operator to be able to respond in near real-time. This means that the IT staff that supports these assets must be able to respond in near real-time if something were to occur.

As a result this group represents the first group of people to really respond to a cyber security event and as a result must maintain such expertise. Cyber security is then a very important

aspect within the SCADA IT group, as this team of people will be required to identify and eradicate such an event in short order in an effort to ensure the reliability of grid operations.

Power generation is much different from the other groups because the generation facilities are many times owned by multiple utilities or entities, with one being the actual operator. As a result generation facilities are beholden to multiple utilities, increasing the stakes associated with their reliable operation. If something fails it could affect a wide range of customers associated with a wide range of utilities. This effectively means that power plants are really further regulated by the utilities themselves, meaning that failure at one can affect many different utilities, requiring a service level agreement between them to ensure that acceptable measures are taken in the event of an incident. These plants then function like mini utilities themselves and maintain IT groups to support the control system within as well as operators to provide command and control over the plants assets. In addition to this, there are various maintenance groups which are responsible for the plants' hard assets such as the turbine, generator, etc. The control system group, like the operators in a control center, monitor the entire plant to ensure that everything functions within normal operating limits. When something fails, they are tasked with dispatching the appropriate maintenance staff in order to correct the problem.

Smart meter groups are concerned with the health and status of the advanced metering infrastructure. They may be required to manage millions of meters, which represents millions of points, one for each customer. These assets are very distributed because customer locations can exist virtually anywhere. A neighborhood of 200 homes for example may represent 200 meters and a number of collectors implemented to support those meters. When you start thinking about on the scale of a large city like Washington DC, you can begin to visualize the scope of the effort, because every household maintains a meter and the group must be able to support reliable operation of the smart meter as well as be able to acquire information related to billing for each customer. They then must be able to bill and support each customer individually, which is a major task given the identified scope.

The smart meter group is then beholden to a set of specific customers who do not really understand how the system works. An outage for example may trigger a number of complaints that may result in action by state and local governments. The point to all of this is that the missions are different amongst the various verticals within the utility; as such the risk is viewed differently. The control center for example views the loss of an application to monitor assets differently from the manner in which the smart metering group views it. The loss of a single

meter for a single customer represents a limited impact to the mission of the smart metering group. But the loss of a system that supports command and control for a plants turbine will have a much larger impact in a power plant. The risk is always relative to the situation, but the key is understanding what the priority of the response will be in each of these verticals. Once this understanding can be established, recovery priorities can be viewed for the utility holistically.

This will allow utilities to better respond to a systematic event caused by a cyber security threat. Meaning that there are various impact levels, some which may affect others, a study to understand this would then represent an understanding of the total impact risk to the utility. Each of these verticals is also constrained by different oversight responsibilities. Smart metering groups for example are likely regulated by state and local governments. Whereas the control center that manages the transmission infrastructure is bound by FERC oversight. A generating plant might be regulated by the Environmental Protection Agency (EPA), FERC, as well as state and local governments. Understanding these impacts and the prioritization of them would be key in the development of a grid risk management strategy.

Short and Long Answer Type Questions

1. Clarify, what do you mean by smart grid?
2. Give the necessity of a smarter grid.
3. Compare the difference between Conventional Grid and Smart Grid.
4. Explain the concept of smart Grid in the power system network.
5. List out the risks in smart grid.
6. Compare smart grid risks versus benefits.
7. Describe the International policies in Smart Grid.
8. Discuss in detail about National Smart Grid Mission(NSGM) in INDIA.
9. Explain the regulatory authorities' role in Indian Power Sector.
10. Describe the privacy information impacts on smart grid.
11. Discuss the security standards available for smart grid.
12. Illustrate the smart grid security strategy in detail.
13. Analyze on smart grid impacts.
14. Explain how security controls frameworks applying to smart grid.
15. Describe how to manage the overall risk to smart grid.
16. Write the necessity of Cyber Security for Smart Grid.
17. Briefly explain the concept of Resilient & Self-Healing Grid.
18. Analyze the Challenges of Smart Grid in a power system network.
19. Discuss the opportunities of smart grid in power system network.

****

2 SMART GRID COMMUNICATIONS AND MEASUREMENT TECHNOLOGY

2.1 COMMUNICATION AND MEASUREMENT

Smart grid communications and measurement technology are critical components of the smart grid infrastructure. These technologies enable real-time monitoring, control, and management of the power grid, allowing for more efficient and reliable energy delivery.

Smart grid communications technology includes a range of wireless and wired communication networks, such as cellular, Wi-Fi, and fiber-optic networks. These networks allow for the transmission of data between different components of the smart grid, such as smart meters, sensors, and control systems.

Smart grid measurement technology includes a variety of sensors and measurement devices, such as smart meters, phasor measurement units (PMUs), and distribution automation systems (DAS). These devices collect data on power consumption, voltage levels, and other parameters in real-time, allowing for more accurate monitoring and control of the power grid.

Smart meters, in particular, are a key component of smart grid measurement technology. These digital devices provide detailed information on energy consumption at the household or business level, enabling consumers to monitor and manage their energy usage more efficiently. Smart meters also allow utilities to better manage energy demand, reduce peak energy usage, and improve billing accuracy.

Overall, smart grid communications and measurement technology play a crucial role in the modernization of the power grid, improving its efficiency, reliability, and sustainability, and helping to create a more resilient and sustainable energy future.

2.1.1 Importance

Because much of the existing transmission and distribution systems in the United States still uses older digital communication and control technology, advanced communication systems for distribution automation, such as Remote Terminal Unit (RTU) and SCADA, are under development as well as innovative tools and software that will communicate with appliances in the home. Ultimately, high-speed, fully integrated, two-way communication technologies will allow the smart grid to be a dynamic, inter- active mega-infrastructure for real-time information and power exchange.

The technology exists for the measure, monitor, and control in real time in the Smart Grid, and this technology plays an essential role in the functioning of the Smart Grid. Issues of standards, cyber security, and interoperability which are dealt with more extensively impact on communication. There is need for the formalization of the standards and protocols which will be enforced for the secured transmission of critical and highly sensitive information within the communications scheme.

Obviously, existing measuring, monitoring, and control technology will have a role in smart grid capability. Establishing appropriate standards, cyber security, and interoperability requires careful study, for example, formalizing the standards and protocols for the secure transmission of critical and highly sensitive information within the proposed communication scheme. Moreover, open architecture's plug-and-play environment will provide secure network smart sensors and control devices, control centers, protection systems, and users. Possible wired and wireless communications technologies can include:

1. Multiprotocol Label Switching (MPLS): high-performance telecommunications networks for data transmission between network nodes
2. Worldwide Interoperability for Microwave Access (WiMax): wireless telecom- munication technology for point to multipoint data transmission utilizing Inter- net technology
3. Broadband over Power Lines (BPL): power line communication with Internet access
4. Wi-Fi: commonly used wireless local area network

Additional technologies include optical fiber, mesh, and multipoint spread spectrum.

The five characteristics of smart grid communications technology are:

1. High bandwidth
2. IP-enabled digital communication (IPv6 support is preferable)
3. Encryption

4. Cyber security
5. Support and quality of service and Voice over Internet Protocol (VoIP)

Reliable intercommunication of hardware and software will require configuring several types of network topologies. Below is a summary of the most likely candidates.

2.1.2. Local Area Network

It consists of two or more components and high-capacity disk storage (file servers), which allow each computer in a network to access a common set of rules. LAN has operating system software which interprets input, instructs network devices, and allows users to communicate with each other. Each hardware device (computer, printer, and so on) on a LAN is a node. The LAN can operate or integrate up to several hundred computers. LAN combines high speed with a geographical spread of 1–10 km. LAN may also access other LANs or tap into Wide Area Net- works. LAN with similar architectures are bridges which act as transfer points, while LAN with different architectures are gateways which convert data as it passes between systems.

LAN is a shared access technology, meaning that all of the attached devices share a common medium of communication such as coaxial, twisted pair, or fiber optics cable. A physical connection device, the Network Interface Card (NIC), connects to the network. The network software manages communication between stations on the system.

The special attributes and advantages of LAN include:

- Resource sharing: allows intelligent devices such as storage devices, programs, and data files to share resources, that is, LAN users can use the same printer on the network; the installed database and the software can be shared by multiple users
- Area covered: LAN is normally restricted to a small geographical area, for example, office building, utility, campus
- Cost and availability: application software and interface devices are affordable and off-the-shelf
- High channel speed: ability to transfer data at rates between 1 and 10 million bits per second
- Flexibility: grow/expand with low probability of error; easy to maintain and operate

LAN topologies define how network devices are organized. The four most common architectural structures are:

1. Bus topology: linear LAN architecture in which transmission from network station

propagates the length of the medium and is received by all other stations connected to it

2. Ring bus topology: a series of devices connected to one another by unidirec- tional transmission links to form a single closed loop
3. Star topology: the end points on a network are connected to a common central hub or switch by dedicated links
4. Tree topology: identical to the bus topology except that branches with multiple nodes are also possible

The devices and software used in LAN utilize a standard protocol such as Ethernet/ IEEE 802.3, Token Ring/IEEE 802.5 or 880.2 (available through IEEE Press).

2.1.3. Home Access Network

It is a LAN confined to an individual home. It enables remote control of automated digital devices and appliances throughout the house. Smart meters, smart appliances and Web-based monitoring can be integrated into this level.

2.1.4. Neighborhood Area Network (NAN)

NAN is a wireless community currently used for wireless local distribution applications. Ideally, it will cover an area larger than a LAN.

- **Bulk generation:** includes market services interface, plant control system, and generators; this domain interacts with the market operations and transmission domains through wide area networks, substation LANs, and the Internet
- **Transmission**: includes substation devices and controllers, data collectors, and electric storage; this domain interacts with bulk generation and operations through WANs and substation LANs; integrated with the distribution domain
- **Distribution:** this domain interacts with operations and customers through Field Area Networks
- **Customer:** includes customer equipment, metering, Energy Management Systems (EMS), electric storage, appliances, PHEVs, and so on
- **Service Providers:** includes utility and third party providers which handle billing customer services, and so on; this domain interacts with operations and customers primarily through the Internet
- **Operations**: includes EMS, Web Access Management System (WAMS), and SCADA; this domain can be sub-divided into ISO/RTO, transmission, and distribution
- **Market:** includes /ISOs/RTOs, aggregators, and other market participants

2.2. MONITORING, PMU, SMART METERS AND MEASUREMENTS TECHNOLOGIES

The smart grid environment requires the upgrade of tools for sensing, metering, and measurements at all levels of the grid. These components will provide the data neces- sary for monitoring the grid and the power market. Sensing provides outage detection and response, evaluates the health of equipment and the integrity of the grid, eliminates meter estimations, provides energy theft protection, enables consumer choice, DSM, and various grid monitoring functions.

With regard to metering and measurement, new digital technologies using two-way communications, a variety of inputs (pricing signals, time-of-day tariff, regional trans- mission organization (RTO) curtailments for congestion relief), a variety of outputs (real time consumption data, power quality, electric parameters), the ability to connect and disconnect, and interfaces with generators, grid operators, and customer portals to enhance power measurement. This is facilitated by the increased utilization of digital electronics for metering and measurements, advancement of the electric meter at the customer level, and installation of wide area monitoring system for advanced utility monitoring and protection. Details of these measurements are discussed in later sections.

New digital technologies will employ two-way communication, a variety of inputs (pricing signals, time-of-day tariffs, RTO) curtailments for congestion relief), a variety of outputs (real-time consumption data, power quality, electric parameters), the ability to connect and disconnect, and interfaces with generators, grid operators, and customer portals to enhance power measurement. This introduces the increased utilization of digital electronics for metering and measurements, advancement of the electric meter at the customer level, and installation of wide area monitoring systems (WAMs) for advanced utility monitoring and protection.

2.2.1. Wide Area Monitoring Systems (WAMS)

WAMS are designed by the utilities for optimal capacity of the transmission grid and to prevent the spread of disturbances. By providing real-time information on stability and operating safety margins, WAMS give early warnings of system disturbances for the prevention and mitigation of system-wide blackouts. WAMS utilize sensors distributed throughout the network in conjunction with GPS satellites for precise time stamping of measurements in the transmission system. The integrated sensors will interface with the communication network. Phasor Measurements are a current technology that is a component of most smart grid designs

2.2.2. Phasor Measurement Units (PMU)

Phasor Measurement Units or Synchrophasors give operators a time-stamped snapshot of the power system. The PMUs consist of bus voltage phasors and branch current phasors, in addition to information such as locations and other network parameters. Phasor measurements are taken with high precision from different points of the power system at the same instant, allowing an operator to visualize the exact angular difference between different locations. PMUs are equipped with GPS receivers which allow synchronization of readings taken at distant points. Microprocessor-based instrumentation such as protection relays and Disturbance Fault Recorders (DFRs) incorporate the PMU module with other existing functionalities as an extended feature. The IEEE standard on Synchrophasors specifies the protocol for communicating the PMU data to the Phasor Data Concentrator.

Figure 2.1 illustrates the PMU measurement system, PMUs ensure voltage and current with high accuracy at a rate of 2.88 kHz. They can calculate real power, reactive power, frequency, and phase angle 12 times per 60 hertz cycle. The actual sampling rate used to achieve this output is 1.4 MHz. Recent trends now require fast controls and online implementations for mitigating voltage collapse in the shortest, least-cost time. Over the years, researchers and engineers have found PMUs are suitable for monitoring and control of voltage stability PMUs).

Offering wide-area situational awareness, phasor measurement work to ease congestion, bottlenecks and mitigate or even prevent blackouts. When integrated with Smart Grid communications technologies, the measurements taken will provide dynamic Visibility into the power system. Adoption of the Smart Grid with real time measurement will enhance every facet of the electric delivery system including generation, transmission, distribution, and consumption. It will increase the possibilities of distributed generation, bringing generation closer to those it serves.

Additional utility monitoring systems include dynamic line rating technology, conductor sensors, insulation contamination leakage current, backscatter radios technology, electronic instrument transformers, and monitors for circuit breaker, cables, batteries, temperature, and current frequency and so on. Research into the application and integration of these measurements into the smart grid is particularly important and continuing work.

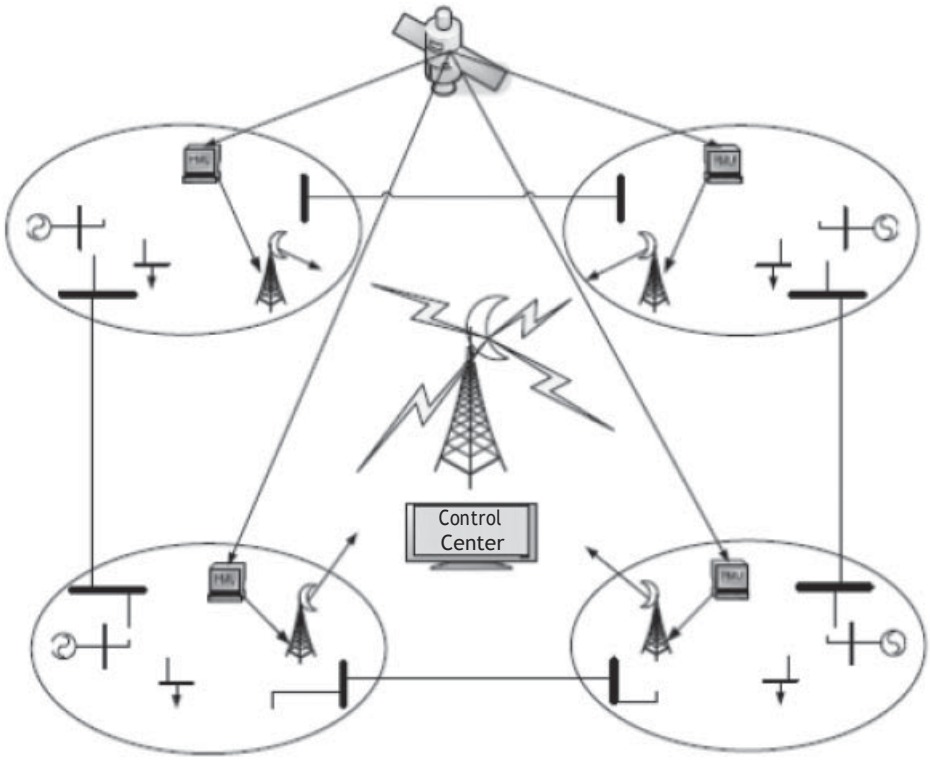


Figure 2.1. Conceptual diagram of a synchronized phasor measuring system

2.2.3. Smart Meters

Smart meters have two functions: providing data on energy usage to customers (end- users) to help control cost and consumption; sending data to the utility for load factor control, peak-load requirements, and the development of pricing strategies based on consumption information and so on Automated data reading is an additional component of both smart meters and two-way communication between customers and utilities. The development of smart meters is planned for electricity, water, and gas consumption.

Smart meters equip utility customers with knowledge about how much they pay per kilowatt hour and how and when they use energy. This will result in better pricing information and more accurate bills in addition to ensuring faster outage detection and restoration by the utility. Additional features will allow for demand-response rates, tax credits, tariff options, and participation in voluntary rewards programs for reduced consumption. Still other features will include remote connect/disconnect of users, appliance control and monitoring, smart thermostat, enhanced grid monitoring, switching, and prepaid metering.

With governmental assistance, large-scale deployment of smart meters has begun throughout the United States. Academic participation in the research and development of metering tools

and techniques for network analysis enhancement and the use of smart meter outputs for voltage stability and security assessment and enhancement have been proposed.

2.2.4. Smart Appliances

Smart appliances cycle up and down in response to signals sent by the utility. The appliances enable customers to participate in voluntary demand response programs which award credits for limiting power use in peak demand periods or when the grid is under stress. An override function allows customers to control their appliances using the Internet. Air conditioners, space heaters, water heaters, refrigerators, washers, and dryers represent about 20% of total electric demand during most of the day and throughout the year [10]. Grid-friendly appliances use a simple computer chip that can sense disturbances in the grid's power frequency and can turn an appliance off for a few minutes to allow the grid to stabilize during a crisis.

2.2.5. Advanced Metering Infrastructure (AMI)

AMI is the convergence of the grid, the communication infrastructure, and the supporting information infrastructure. The network-centric AMI coupled with the lack of a composite set of cross industry AMI security requirements and implementation guidance, is the primary motivation for its development. The problem domains to be addressed within AMI implementations are relatively new to the utility industry; however, precedence exists for implementing large-scale, network-centric solutions with high information assurance requirements. The defense, cable, and telecom industries offer many examples of requirements, standards, and best practices that are directly applicable to AMI implementations.

The functions of AMI can be subdivided into three major categories:

- **Market applications**: serve to reduce/eliminate labor, transportation, and infra- structure costs associated with meter reading and maintenance, increase accuracy of billing, and allow for time-based rates while reducing bad debts; facilitates informed customer participation for energy management.

Customer applications: serves to increase customer awareness about load reduction, reduces bad debt, and improves cash flow, and enhances customer convenience and satisfaction; provides demand response and load management to improve system reliability and performance

Distribution operations: curtails customer load for grid management, optimizes network based on data collected, allows for the location of outages and restoration of service, improves customer satisfaction, reduces energy losses, improves performance in event of outage with reduced outage duration and optimization of the distribution system and distributed generation management, provides emergency demand response

An extension of AMI will be smart meters which handle customers' gas and water usage data. The issues associated with ensuring network and data security.

2.3. GIS AND GOOGLE MAPPING TOOLS

GIS is useful for managing traditional electric transmission and distribution and telecom networks. It can also help to manage information about utility assets for data collection and maintenance.

Google's free downloadable Google Earth software offers geographical contextual information in an updated user-friendly platform that facilitates inquiry-based study and analysis. Users can create and share many types of dynamically-updating data over the Internet. Keyhole Markup Language (KML) allows them to overlay basic data types such as images, point data, lines, and polygons. Through satellite imagery, maps are available from space to street-level. The integration of GIS with Google Earth or other mapping tools will aid in understanding the relationship of the grid network to its surroundings, for example, determining the optimal location of rights of way, placement of sensors and poles, and so on. GIS technology will provide partial context to operators and planners, for example, real-time sensors that collect the data needed to reconfigure networks for reducing outages and equipment failures.

The trends in the development of the electric power system and the expectation of future demand suggest the following needs:

- Reducing outage time
- Preventing power theft which causes significant unaccounted losses
- Effective system for collection and billing system
- Expanding services for customers
- Effective asset management
- Improving reliability such as SAIDI (System Average Interruption Duration Index) and SAIFI (System Average Interruption Frequency Index) for distribution networks
- Improving analysis of customer complaint logs

- Enhancing load flow power quality analysis and fault study for current and anticipated problems
- Scheduling of actions such as load shedding and vegetation control

2.4 MULTIAGENT SYSTEMS (MAS) TECHNOLOGY

Google's free MAS are a computational system in which several agents cooperate to achieve a desired task. The performance of MAS can be decided by the interactions among various agents. Agents cooperate to achieve more than if they act individually.

Increasingly, MAS are the preferential choice for developing distributed systems. The development of monitoring and measurement schemes within the smart grid environment can be enhanced through the use of MAS architecture (Fig. 2.2). As an example, MAS have been utilized as a detection and diagnosis device and in system monitoring.

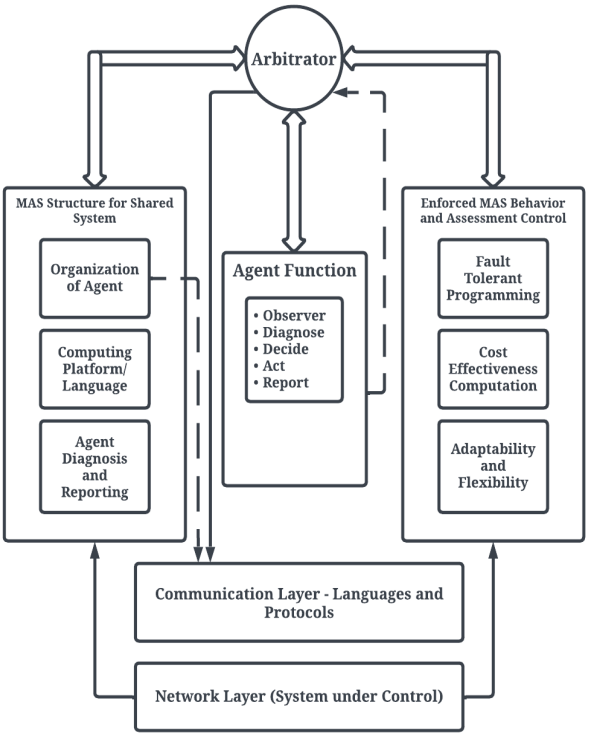


Figure 2.2. Simplified multiagent architecture

Such architectures utilize a collection of agents such as Arbitrator Agents (AA), System Monitoring Agents (SMA), Fault Detection Agents (FDA), Diagnosis Agents (DA), a Judgment Index Agent (JIA), and a Scheduling Agent (SA)

Information passes between the agents about the appropriate actions to be taken. When implemented, the process repeats itself to constantly monitor the system so that management of system conditions can be implemented instantaneously.

2.4.1. Multiagent Systems for Smart Grid Implementation

The DOE's Modern Grid Initiative explains that a smart grid integrates advanced sensing technologies, control methods, and integrated communications into the present electricity grid at both transmission and distribution levels. The smart grid is expected to have the following key characteristics:

1. self-healing
2. consumer friendly
3. attack resistant
4. provide power quality for 21st-century needs
5. accommodate all generation and storage options
6. enable markets
7. optimize assets and operate efficiently

Central to the operation of any power system is its control architecture consisting of hardware and software protocols for exchanging system status and control signals. In conventional electric power systems, this is accomplished by SCADA. Current trends to control and monitor system operations are moving toward the use of MAS. A multi agent system is a combination of several agents working in collaboration pursuing assigned tasks to achieve the overall goal of the system. The multiagent system has become an increasingly powerful tool in developing complex systems that take advantages of agent properties: autonomy, sociality, reactivity and pro-activity.

The multiagent system is autonomous in that they operate without human interventions. The multiagent system is sociable in that they interact with other agents via some kind of agent communication language. The agents also perceive and react to their environment. Lastly, the multiagent system is proactive in that they are able to exhibit goal oriented behavior by taking initiatives.

2.4.2. Multiagent Specifications

In this section, the specifications of a control agent, a distributed energy resource (DER) agent, a user agent, and a database agent in the Intelligent Distributed Autonomous Power System (IDAPS) MAS are defined

1. Control agent: responsibilities include monitoring system voltage and frequency to detect contingency situations or grid failures, and sending signals to the main circuit breaker to isolate the IDAPS microgrid from the utility when an upstream outage is

detected; receiving electricity price ($/kWh) signal from the main grid, which may be obtained from AMI, and publishing them to the IDAPS entities

2. DER agent: responsibilities include storing associated DER information, monitoring and controlling DER power levels and connect/disconnect status; DER information to be stored may include DER identification number, type (solar cells, microturbines, fuel cells), power rating (kW), local fuel availability, cost function or price at which users agree to sell, DER availability, that is, planned maintenance schedule

3. User agent: acts as a customer gateway that makes features of an IDAPS microgrid accessible to users; responsibilities include providing users with real- time information on entities residing in the IDAPS system; monitors electricity consumption by each critical and noncritical load; allows users to control the status of loads based on user's predefined priority

4. Database agent: serves as a data access point for other agents as well as users; responsibilities include storing system information, recording messages and data shared among agents.

2.4.3. Multiagent Technique

An agent of a MAS may be defined as an entity with attributes considered useful in a particular domain. In this framework, an agent is an information processor that performs autonomous actions based on information. Common agent attributes include:

- Autonomy: goal-directedness, proactive and self-starting behavior
- Collaborative behavior: the ability to work with other agents to achieve a common goal
- Knowledge-level communication ability: the ability to communicate with other agents with language resembling human speech acts rather than typical symbol-level program-to-program protocols
- Reactivity: the ability to selectively sense and act
- Temporal continuity: persistence of identity and state over long periods

MAS can be characterized by:

- Each agent has incomplete capabilities to solve a problem
- No global system control

- Decentralized data
- Asynchronous computation

For instance, the system outage of a ship could be caused by an internal system error or any external contingency from battle. To pursue the best ship performance, it is very important to restore the electric power supply as much as possible. When a fault occurs on the ship power system, the protection systems will isolate the fault from the remaining power grid. Then the system should restore the electric power to a target configuration after the outage. An example of MAS architecture in action is a power failure on board a ship that is caused by an internal system error, an external contingency from battle, and so on.

Clearly, the goal is rapid restoration of the onboard power supply; hence, when a fault occurs, the protection system will isolate the fault, allowing the system to restore power to a target configuration after the outage.

2.5. Microgrid and Smart Grid Comparison

The following table 2.1 gives the comparison between micro grid and smart grid.

Table 2.1 Comparison of Microgrid versus Smart Grid

Microgrid	Smart Grid
Micro grid is **interconnected loads + DERs** within a clearly defined electrical and geographical boundaries which acts as a single controllable entity with respect to the main grid.	Smart grid is any **electrical grid +ICT/IT/Sensor Technology all levels.**
Microgrid = Small smart grid	Smart Grid = smart macro grid (utility grid)
Micro grid can be Considered as a sub set of smart grid	Smart grid can be composed from a number of microgrids.
Micro grid permits distributed generation at small scale as compared to smart grid.	Smart grid permits distributed generation at large scale as compared to Microgrid.
It considers the utilization of distributed energy systems in order to improve the reliability and flexibility of the electricity	It aims to combine intelligent technologies with electricity to improve the convenience and reliability of whole electricity.
Installation cost is economical	Installation cost is very high
It is a small-scale power supply network that is designed to provide for a small community.	It is a large-scale power supply network that is designed to provide power for a big

	community.
It enables local power generation for local loads.	It enables local power generation for local as well as outstation loads.
Size of the microgrid may range from housing estate to municipal regions.	Size of the smart grid always bigger than municipal regions.
Small substations at individual microgrid, monitor and controls power distribution using Microprocessor based automatic load shedding controller.	Distribution of total generation carried out economically along with LDC (Load Dispatch Centre).
Microgrids are smaller scale, require fewer decision makers and have faster implementation.	Smart grids operate at the utility and national grid level, involving the large transmission and distribution lines.

Short and Long Answer Type Questions

1. List out the Characteristics of smart grid communications technology.
2. Write the role of HAN in smart grid.
3. Give the role of LAN in smart grid.
4. Write the role of NAN in smart grid.
5. Analyze the Broadband over Power line (BPL) in Smart Grid.
6. Define the term Phasor Measurement Unit. (PMU)
7. List out the applications of Phasor Measurement Unit (PMU) in Smart Grid.
8. Explain the concept of phase measuring unit (PMU) with neat block diagram.
9. Define the term Smart Meters in the smart grid.
10. List out the Advantages of Smart Meters in Smart Grid.
11. Give the Need of Smart Meters in the Smart Grid.
12. Compare between Conventional Meter and Smart Meter.
13. Discuss the importance of Wide area network in smart grid.
14. Explain the Building Blocks of AMI in the smart Grid.
15. Write the importance of GIS and Google mapping tools in smart grid.
16. Define Multiagent system (MAS) technology.
17. Explain in detail about Multiagent system (MAS) technology.
18. Compare micro grid and smart grid.

3 PATHWAY FOR DESIGNING SMART GRID

3.1. INTRODUCTION TO SMART GRID PATHWAY DESIGN

Smart grid pathway design is the process of planning and implementing the modernization of the electricity grid to create a more efficient, reliable, and sustainable power system. This process involves identifying the goals and objectives of the smart grid project, assessing the current state of the power grid, designing the technical infrastructure and communication systems, and implementing the necessary changes.

The pathway design process begins with a comprehensive analysis of the current power grid infrastructure, including the generation, transmission, and distribution systems. This analysis involves assessing the condition and capacity of the existing infrastructure, identifying potential bottlenecks, and evaluating opportunities for improvement.

Once the current state of the power grid has been assessed, the next step is to define the goals and objectives of the smart grid project. These may include improving energy efficiency, integrating renewable energy sources, enhancing grid resilience, reducing energy waste, and improving the reliability and security of the power grid.

The pathway design process also involves the selection and design of the technical infrastructure and communication systems necessary for the modernization of the power grid. This may include the selection of smart meters, sensors, and control systems, as well as the design and implementation of communication networks, data management systems, and other technologies required for real-time monitoring and control of the power grid.

Finally, the implementation phase of the pathway design process involves the installation and integration of the new infrastructure and communication systems, as well as the training of personnel to operate and maintain the new equipment and systems.

Overall, the goal of smart grid pathway design is to create a more efficient, reliable, and sustainable power system that can meet the changing needs of consumers and the demands of the 21st century energy landscape.

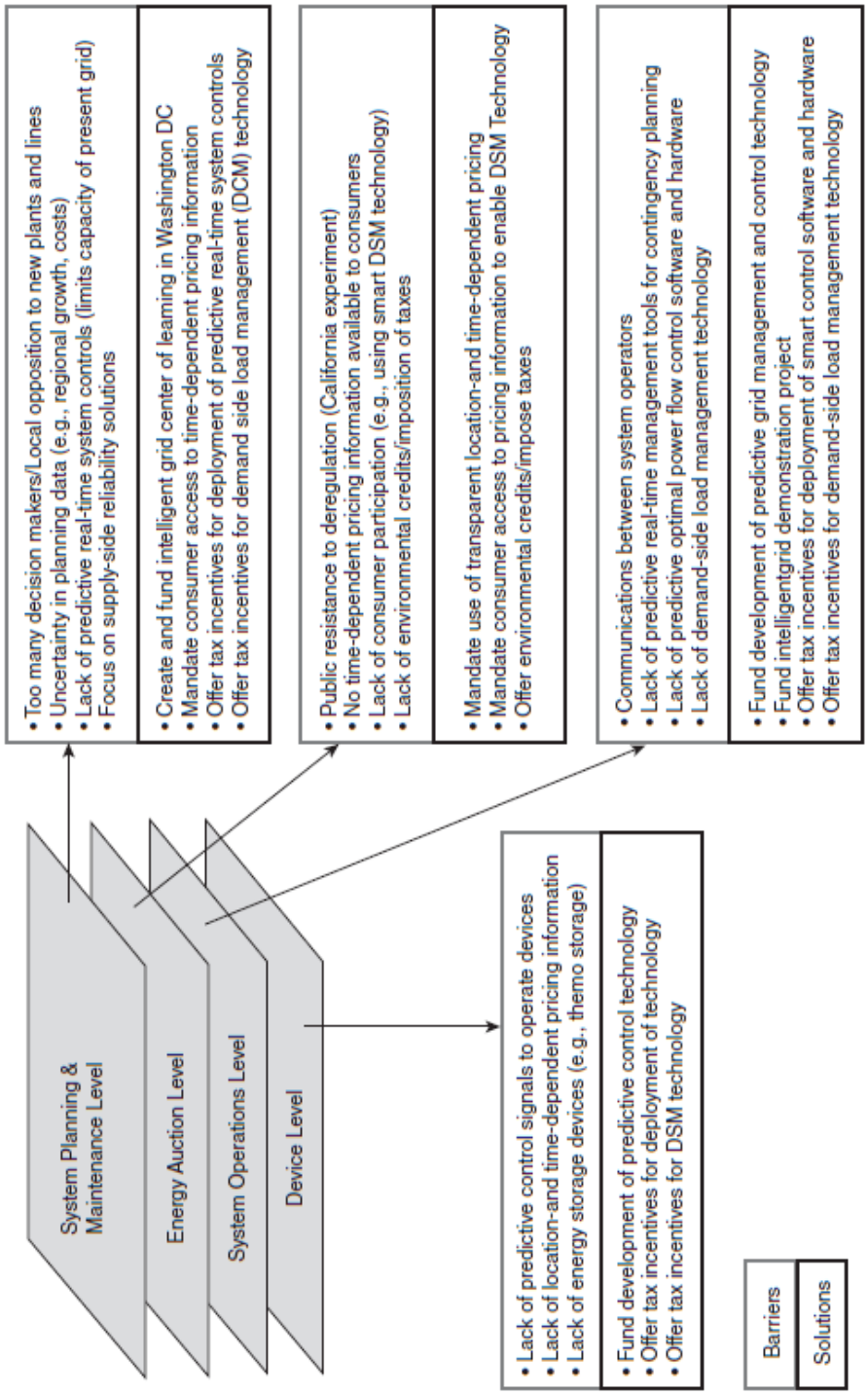

System Planning & Maintenance Level
Energy Auction Level
System Operations Level
Device Level
• Too many decision makers/Local opposition to new plants and lines
• Uncertainty in planning data (e.g., regional growth, costs)
• Lack of predictive real-time system controls (limits capacity of present grid)
• Focus on supply-side reliability solutions
• Create and fund intelligent grid center of learning in Washington DC
• Mandate consumer access to time-dependent pricing information
• Offer tax incentives for deployment of predictive real-time system controls
• Offer tax incentives for demand side load management (DCM) technology
• Public resistance to deregulation (California experiment)
• No time-dependent pricing information available to consumers
• Lack of consumer participation (e.g., using smart DSM technology)
• Lack of environmental credits/imposition of taxes
• Mandate use of transparent location-and time-dependent pricing
• Mandate consumer access to pricing information to enable DSM Technology
• Offer environmental credits/impose taxes
• Communications between system operators
• Lack of predictive real-time management tools for contingency planning
• Lack of predictive optimal power flow control software and hardware
• Lack of demand-side load management technology
• Fund development of predictive grid management and control technology
• Fund intelligentgrid demonstration project
• Offer tax incentives for deployment of smart control software and hardware
• Offer tax incentives for demand-side load management technology
• Lack of predictive control signals to operate devices
• Lack of location-and time-dependent pricing information
• Lack of energy storage devices (e.g., thermo storage)
• Fund development of predictive control technology
• Offer tax incentives for deployment of technology
• Offer tax incentives for DSM technology
Barriers
Solutions

Figure 3.1. Barriers and solutions to the smart grid

3.2. BARRIERS AND SOLUTIONS TO SMART GRID DEVELOPMENT

Figure 3.1 illustrates the multilayered approach to designing the smart grid. The layers or levels are:

1. System Planning and Maintenance
2. Energy Auction
3. Systems Operations
4. Device

System Planning and Maintenance Level:

Issues include too many decision-makers, local opposition to new plants and lines, planning uncertainties, lack of predictive real-time system controls, and not enough focus on supply-side reliability solutions.

To overcome these barriers, the smart grid design needs consumer access to time- dependent pricing information, tax incentives for deployment of predictive real-time system controls, and tax incentives for DSM technologies. The solution method will:

- Create and fund an intelligent grid center of learning
- Mandate consumer access to time-dependent pricing information
- Offer tax incentives for deployment of predictive real-time system controls
- Offer tax incentives for DSM
- These solutions should minimize maintenance at the level of implementation.

Energy Auction Level: Issues include public resistance to deregulation, inadequate time-dependent pricing information unavailable to consumers, lack of consumer participation (for example, using smart DSM technology), and lack of environmental credits/imposition of taxes. The solution will

- Mandate use of transparent location-and-time-dependent pricing
- Mandate consumer access to pricing information to enable DSM technology
- Offer environmental credits/impose taxes

Energy auction level (EAL) purports to redefine pricing structure for the energy market. This will go a long way toward making the accessibility and usage of the grid afford- able by the general populace.

System Operation Level: Issues include communication pitfalls among system operators to handle emergencies, lack of predictive real-time management tools for efficient handling, and lack of predictive optimal power flow control software and hardware and DMS technology.

The solution will:

- Fund development of predictive grid management and control technology
- Fund intelligent demonstration projects
- Offer tax incentives for deployment of smart control software and hardware
- Offer tax incentives for DSM technology

Device Level: Issues include lack of predictive control signals to operate devices, lack of locational pricing and time-dependent pricing information, and lack of energy storage devices.

The solution will:

- Fund development of predictive control technology
- Offer tax incentives for deployment of technology
- Offer tax incentives for DSM technology

3.3. SOLUTION PATHWAYS FOR DESIGNING SMART GRID USING ADVANCED OPTIMIZATION AND CONTROL TECHNIQUES FOR SELECTION FUNCTIONS

Electric power grids are highly complex dynamical systems vulnerable to a number of disturbances in day-to-day operations. Random disturbances from weather and accidents rarely produce wide area catastrophic failures. However, the availability of detailed real-time operational data opens the door for maliciously designed disturbances. Figure 3.2 illustrates the four advanced optimization and control techniques required to meet the criteria for smart grid performance.

3.4. GENERAL LEVEL AUTOMATION

Automation at this level involves the use of addressed computation technologies and a new algorithm for dispatch and unit commitment to ensure:

- Reliability
- Stability
- Optimal dispatch
- Unit commitment under different uncertainties and constraints
- Security analysis
- Distributed generation control

Forecasting techniques must be incorporated into real-time operating practices as well as day-to-day operational planning, and consistent and accurate assessment of variable generation availability to serve peak demand is needed in longer-term system planning. High-quality and real-time data must be integrated into existing practices and software. The electricity industry is being encouraged to pursue research and development in these areas

3.4.1 Reliability

Power system reliability is defined as the ability to deliver electricity to all points of power utilization within acceptable standards. The traditional reliability analysis methods are deterministic, for example, n-1 criterion where the system is deemed reliable if it can operate under a single unplanned outage, whereas in the smart grid environment, reliability analysis may not be used for extreme events. Thus, a new reliability and sustainability metric should be capable of handling:

- Nonlinearity of the system parameters, especially in the presence of the new mix of generation resources (wind, storage, hydro, and so on) and high power conversion devices
- Uncertainty in load demand and generation availability that are functions of time and contingencies
- System dynamics that reflect the market, availability of natural resources, network reconfiguration, and load switching
- Stochasticity of the system parameters due to man-made or natural events over different time-scales of operations

Indices such as loss of load probability (LOLP) and expected unserved energy (EUE) are used to determine the energy/load that can be supplied over time for different reliability services. The cost component balances the cost of reliability improvements with the cost of service disruptions. The ultimate goal is to achieve the maximum reliability under a variety of probable contingencies. Autonomous control actions will serve to meet this goal.

3.4.2 Stability

Power system stability is the ability of the bulk power electric power system to with- stand sudden disturbances such as electric short circuits or unanticipated loss of system components . At the generation level, transient stability is the primary consideration; as the system expands, the significance of transient stability increases.

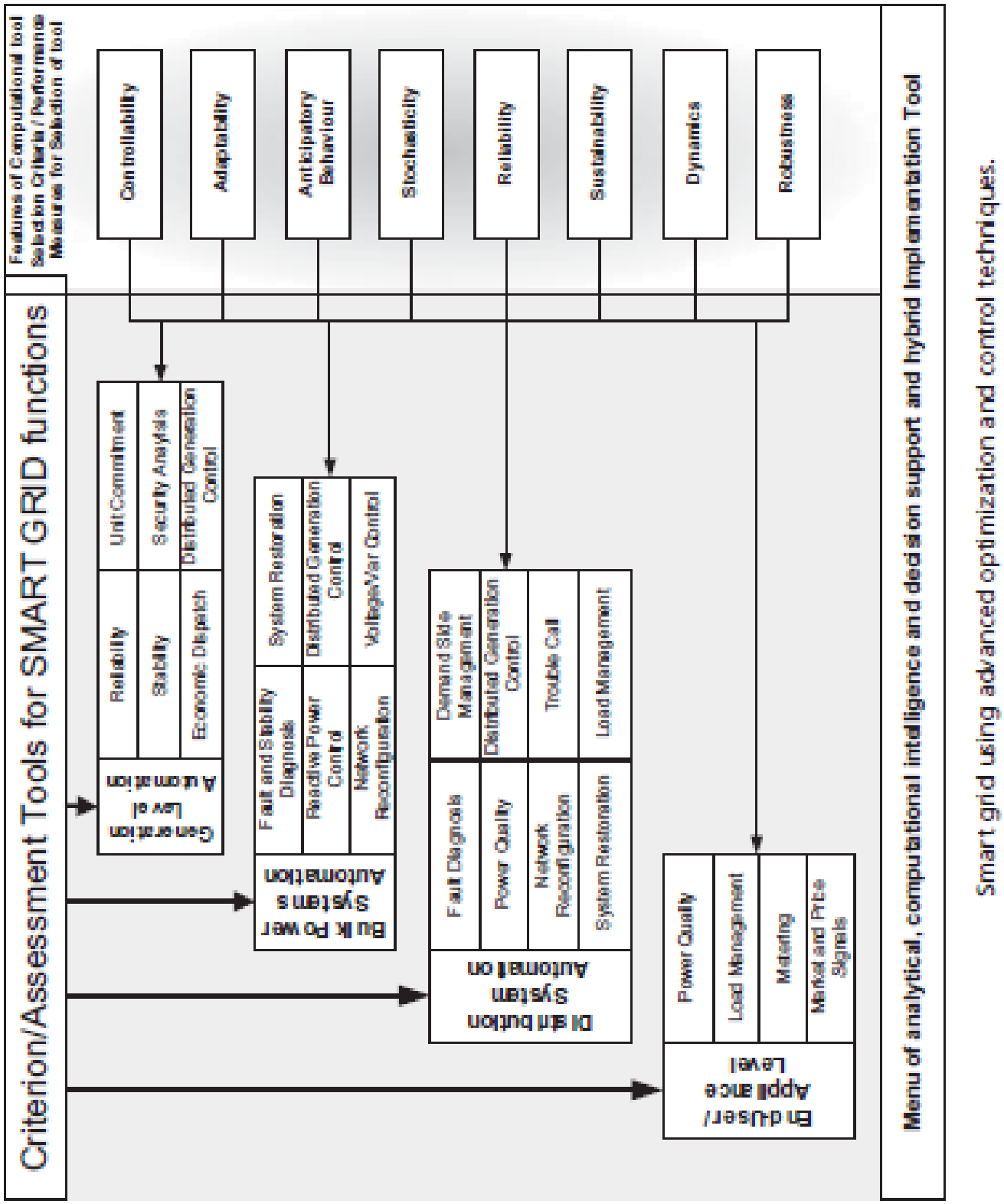


Figure 3.2. Smart grid using advanced optimization and control techniques

In general, voltage and angle stability assessments are needed to ensure dynamic reconfiguration in response to system faults and disturbances. The methods discussed earlier

are conventional analytical methods including risk assessment and Lyapunov stability assessment. Since the margin of stability cannot be obtained using numerical methods, an energy-based method has been utilized for angle stability. Traditional methods for solving stability problems, including continuation power flow method, singular value decomposition, Jacobian condition number, and energy margin methods are generally used, but all are based on offline studies.

WAMS and PMU measurements prepared for the smart gird environment will allow for the real-time evaluation of the system under different loading and unknown contingencies. Advancements in stability studies aim to address the impacts of contingency with the help of developing new indices for stability assessment.

3.4.3 Economic Dispatch

Economic dispatch is a computational process where the total required generation including renewable energy resources is distributed among the generation units in operation by minimizing the selected cost criterion subject to load and operational constraints. For any specified load condition, the output of each plant (and each generating unit within the plant) which will minimize the overall cost of fuel needed to serve the system load is calculated. Traditionally, the economic dispatch problem is formulated as an optimization with cost as the quadratic objective function:

$$F(P_g) = \sum_{i=1}^{N_g} \left(\alpha_i + \beta_i P_{g_i} + \gamma_i P_{gi}^2\right)$$

$$\sum_{i=1}^{N_g} P_{g_i} - \sum_{i=1}^{N_D} P_{D_i} + P_{loss} = 0$$

$$\text{s.t } V_{\min} \le V \le V_{\max}$$

$$P_{g\min} \le P_g \le P_{g\max}$$

The constraints include equalities and inequalities which represent the power equations as well as generator, bus, voltage, and line flow limits. This can be solved using analytical mathematical programming such as NLP, QP, LP, Newton method, interior point methods (IPM), and decision support methods such as AHP.

Computational methods used to solve this form of problem require simplifications of the objective function to be piecewise linear and monotonically increasing, for solution, but they suffer from the power system's problem of nonconvexity behavior which then leads to local

minimization or local optimality. Alternative solution methods such as (EP), GA, tabu search, neural networks, particle swarm optimization, and ADP are proposed for improving the performance of the economic dispatch algorithm.

3.4.4 Unit Commitment (UC)

UC, an operation scheduling function, is sometimes termed "predispatch." In the overall hierarchy of generation resources management, the UC function coordinates economic dispatch and maintenance and production scheduling over time. UC scheduling covers the scope of hourly power system operation decisions with a one-day to one- week horizon.

The UC decisions are coupled or iteratively solved in conjunction with coordinating the use of hydro units including pumped storage with capabilities and to ensure system reliability. The function may also include labor constraints due to normal crew policy that a full operating crew will be available without committing to overtime costs. A prime consideration is the adoption of environmental controls, such as fuel switching. The application of computer-based UC programs by electric utilities has been slow due to the following reasons:

i. They are not readily transferred between systems. The problem is so large and complex that only the most important features can be included; these vary among systems, thus requiring tailor-made applications.
ii. Political problems, constraints, and peculiarities of systems that are not easily amenable to mathematical solutions and may be difficult to model.
iii. Operating situation changes quickly; there is so much objective and subjective information about the system that the input requirements of sophisticated, computerized schedulers are discouraging.
iv. As in other computer applications areas, developing fully workable systems has been difficult; building an operator's confidence is also difficult.

The UC schedule is obtained by considering:

- Unit operating constraints and costs
- Generation and reserve constraints
- Plant startup constraints
- Network constraints

Formulation of Unit Commitment. To account for constraints, randomness, and stochastic variables, several assumptions are needed for the formulation of UC. Several classifications for reserve include units on spinning reserve and units on cold reserve under the conditions

of banked boiler or cold start part of the formulation. The first constraint to be met is that net generation must be greater than or equal to the sum of total system demand and required system reserve:

$$\sum_{i=1}^{N} P_{g_i}(t) \geq (\text{Net Demand} + \text{Reserve})$$

In case the units should maintain a given amount of reserve, the upper bounds must be modified accordingly. Therefore:

$$P_{gi}^{\max} = P_{gi}^{capacity} - P_{gi}^{reserve}$$

$$Demand + Losses \leq \sum_{i=1}^{N} P_{g_i} - \sum_{i=1}^{N} P_{g_i}^{reserve}$$

$$C_{cold} = C_O(1 - e^{\alpha t}) + C_L$$

where

C_{cold}: Cost to start an off-line boiler

α: Unit's thermal time constant;

t: Time in seconds

C_L: Labor cost to up the units

C_O: Cost to start up a cold boiler

$C_{banked} = C_B t + C_L$

Where

C_B: Cost to start up a banked boiler

t: Time in seconds

Additional constraints include uncertainty and some of the security index or vulnerability index and congestion margin used in the formulation of the UC system for a smart grid.

Lagrangian relaxation is among the classical techniques used for the UC problem where the constraints are based on stochastic variables and predictivity is considered. The stochastic optimization method is useful for solving this problem as its randomness is a good solution approach, but its predictivity is not as good compared to ADP. ADP can handle discrete systems which use computational techniques and IPM as features of the more recent techniques which have been able to handle stochastic and dynamics indices.

3.4.5 Security Analysis

Power system security analysis detects whether the power system is in a secure state or an alert state. Secure state implies that the load is satisfied and no limit violations will occur under the current operating conditions and in the presence of unforeseen contingencies. Alert state implies that particular limits are violated and/or the load demand cannot be met, and corrective actions are necessary to bring the system back to the secure state.

Dynamic analysis evaluates the time-dependent transition from the precontingent to the postcontingent state. Dynamic security has been analyzed either by deriving dynamic security functions only, or along with the development of some preventive action techniques. Traditionally, n-1 contingency analysis has been used for the evaluation of security defined as the system's ability to supply load under contingency.

The combination of computational intelligence and NP provides an improved security assessment which accounts for randomness or stochasticity in the data. The index for measuring security is based on real-time measurements. An example of the new indices to estimate system performance is vulnerability which could be based on loss of load index, voltage index, or powerflow index.

3.5 BULK POWER SYSTEMS AUTOMATION OF THE SMART GRID AT TRANSMISSION LEVEL

The automation of different functions of the bulk grid level of the transmission system is important for achieving resilience and sustainability of the system. The following functions are evaluated, and the appropriate intelligent technology is proposed:

- Real-time angle, voltage stability, and collapse detection and prevention via intelligent-based data
- Reactive power control based on intelligent coordination controls
- Fault analysis and reconfiguration schemes based on intelligent switching operations
- Power generation and load balance via intelligent switching operation and minimizing demand interruption
- DG and DSM via DR strategy for peak shaving, including increased proliferation and control of RER

The integration of these functions is shown in Figure3.3. Some of the functions and roles are presented next.

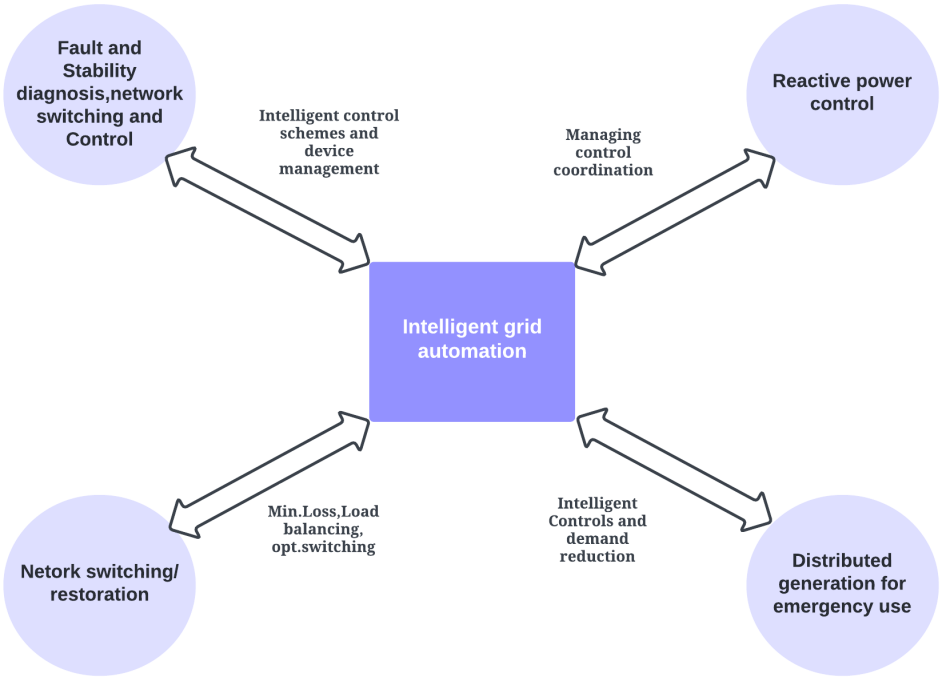

Fault and Stability diagnosis,network switching and Control
Intelligent control schemes and device management
Reactive power control
Managing control coordination
Intelligent grid automation
Netork switching/ restoration
Min.Loss,Load balancing, opt.switching
Intelligent Controls and demand reduction
Distributed generation for emergency use

Figure3.3. Intelligent grid automation

3.5.1 Fault and Stability Diagnosis

Voltage and angle stability assessments ensure dynamic reconfiguration in response to system faults and disturbances. Since the margin of stability cannot be obtained using numerical methods, an energy-based method has been proposed for angle stability. To date, real-time evaluation of the system under different loading and unknown contingencies has not been implemented. Analytical techniques used for fault analysis include the circuit theory-based method and the traveling wave-based method. Methods for detection of voltage instability are generally based solely on local measurements of voltage, for example under voltage load shedding (UVLS). WAM and PMUs also play a major role in stability monitoring and analysis

3.5.2 Reactive Power Control

The main factor causing instability is the inability of the power system to meet the demand for reactive power. The heart of the problem is usually the voltage drop that occurs when active power and reactive power flow through the inductive reactance associated with the transmission network. Reactive power control uses optimization techniques to minimize loss and schedule reactive resources to remove the voltage degradation problem. The use of real-time power margin as a constraint in optimization can be solved in real time with intelligent optimization techniques based on DSOPF.

Other functions such as network switching and restoration use knowledge based systems completed with GA and fuzzy logic to select the outage units and lines and appropriate control measures. For scheduling outages. ADP and other variants of EP, such as GA and ACO, are adapted to address RER penetration into the smart grid and to manage variability.

3.6 DISTRIBUTION SYSTEM AUTOMATION REQUIREMENT OF THE POWER GRID

Distribution automation and control involves the delivery of energy to customers. Figure 3.4 shows the distribution automation schemes for distribution systems.

Smart Distribution solutions are designed to minimize energy losses, mitigate power disruptions, and optimally utilize distributed smart grid components, including alternative energy sources, power storage, and PHEV charging infrastructure.

Greater access to larger pools of available generation and demand may also be important to the reliable integration of large-scale variable generation. As the level of variable generation increases in a balancing area, the resulting variability may not be manageable with its existing conventional generation resources. Base load generation may need to be frequently cycled in response to these conditions, which introduces reliability concerns as well as economic consequences. These efforts may also help to address minimum load requirements of conventional generation and contribute to the effective use of off-peak, energy-limited resources

3.6.1 Voltage/VAr Control

Voltage control within a specified range of limits and capacitor switching is an effective means of minimizing loss, improving voltage profiles, and deferring construction in the end within the reliability and power quality constraints.

Voltage/VAr Control considers a multiphase unbalanced distribution system operation, dispersed generation, and control equipment in the large system. In distribution automation, functions using voltage/VAr control options must maintain proper communication throughout decision-making to install capacitors, thereby realizing the cost benefit ***Formulation of Voltage/VAr Problem.***

This includes integrating voltage/VAr with the load management problem to improve efficiency. The objectives are:

a. Customer Outage Cost

$$\text{Min Outage Cost} = \sum \left(X_{ik} \cdot PC_{ki} \cdot CC_k \right)$$

Where

X_{ik}: Level of Curtailable Load Selection of type k at bus i (p.u. MW)

PC_{ki}: Max Curtailable MW of type k at the ith bus (p.u. MW)

CC_k: Curtailment Cost of Customer Type k ($/p.u. MW)

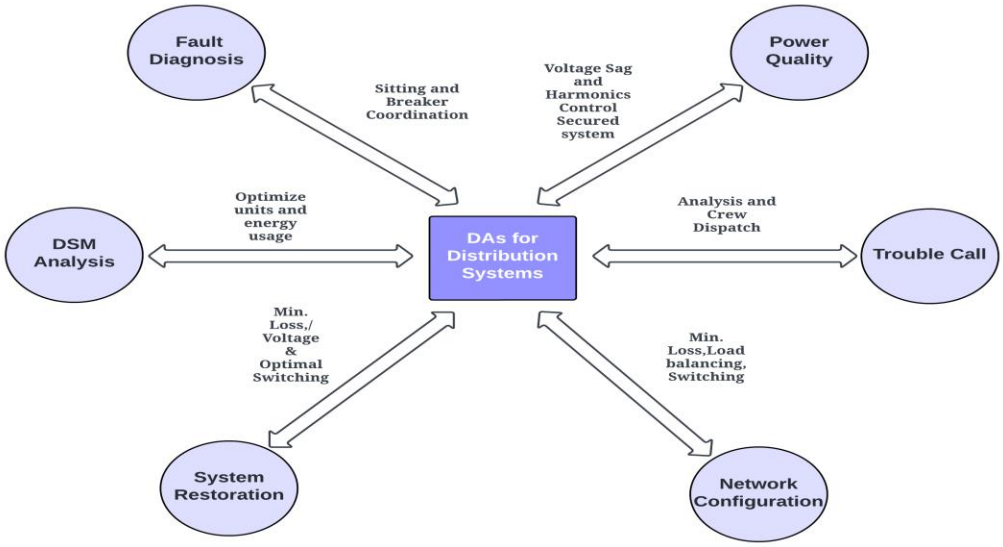


Figure 3.4. Distribution automation for distribution systems

b. Loss Minimization

The objective of the loss minimization function is given by:

$$\text{Min } I^2 r = \sum_{ij} r_{ij} \frac{P_{ij}^2 + Q_{ij}^2}{|V_i|^2}$$

c. Load Balancing

$$Max \frac{S_i}{S_{i\max}}$$

Where:

N: Total number of buses

P_{ij}, Q_{ij}: Transfer Power (branch i-j at p.u.)

V_i: Voltage of bus i (p.u.)

d. Multiple objective functions

$$Z = Min[a + b - c]$$

System Operating Constraints include:

a. Branch Flow Equations

$$Y_{i+1} = f_{i+1}(Y_i)$$

where $Y_i = [P,Q,|V|^2,X_k,Q_s,\delta_i]$

Branch flow considers the recursive relationships between the successive nodes in the radial distribution system. The demand in PD, QD has an interruptible component which is the load management control options X. In addition, the reactive power equation has the capacity switching option Qs.

b. Voltage Limits/Current Limits

The voltage and current limits are given as:

$$\left|V_i^{\min}\right| \le \left|V_i\right| \le \left|V_i^{\max}\right|$$

$$\left|I_{ij}^{\min}\right| \le \left|I_{ij}\right| \le \left|I_{ij}^{\max}\right|$$

c. Capacitor Control Limits

$$Qs_i^{\min} < Qs_i \le Qs_i^{\max}$$

d. Curtailable Load Control Limits

$$P_i \times X_{ki} \le Pc_{ki}$$

$$Q_i \times X_{ki} \le Qc_{ki}$$

3.6.2 Power Quality

Power quality is the ability of a system to operate without causing disturbance or damage to loads and components. Power quality is a major concern because of the sensitivity of digital and modern control equipment to distortion/PQ deterioration. A basic requirement for maintaining power quality is balancing supply and demand. Typical indices utilized as power quality measures include:

- Voltage transient impulse
- Voltage sag
- Total harmonic distortion
- Flicker factor

A complete listing of quality measures employed in the global electric power industry is given in Table 3.1.

Several accepted power quality standards which apply to electrical distribution systems are itemized in "Voltage Disturbances Standard EN 50160: Voltage Character- istics in Public Distribution Systems." A real-time power quality study features several aspects:

TABLE 3.1. Typical Power Quality Indices

Phenomena Indices	Calculations	Parameters	Networks/Systems where index is applied
Voltage Sag or Swell	$\Delta V = \lvert V_i - V_{nom} \rvert$	V_i—voltage at bus i V_{nom}—nominal voltage	Networks which feature: Remote System Faults
Flicker factor	$FF = \frac{\Delta V}{\lvert V \rvert}$	V—voltage	Networks which feature: Intermittent loads Motor starting Arc Furnaces
Total Harmonic Distortion (THD)	$THD = \frac{\sqrt{\sum_{i=2}^{\infty} \left(I^{(i)}\right)^2}}{I^{(1)}}$ $THD = \frac{\sqrt{\sum_{i=2}^{\infty} \left(V^{(i)}\right)^2}}{V^{(1)}}$	$I^{(i)}$—i^{th} harmonic current $V^{(i)}$—i^{th} harmonic voltage	Networks which feature: Non-linear loads System resonance

1. Sensitive detection of power disturbances
2. Real-time measurement of parameters of signal components in power disturbances
3. Quantification of power disturbances and their negative impacts on power systems
4. Identification of types and causes of power disturbances
5. Location of power disturbances

Power quality monitoring and analysis in the smart grid will utilize real-time data.

3.6.3 Network Reconfiguration

Cost-effective reconfiguration assessment strategies are needed to address the following challenges:

- Nonlinearity of power system parameters
- Uncertainty in load demand and generation availability
- System dynamics
- Stochastic of system parameters

Intelligent control methods including adaptive critics designs, fuzzy logic, and ANN methods may provide adaptive stochastic solutions to the general problem formulation.

3.6.4 Demand-Side Management

DSM is an effective means of modifying customer demand to reduce operating expenses from expensive generators and defer capacity addition in the long run. Environmental conservation is improved with DMS options, which also sustain industrialization at minimum cost. In addition DSM options provide reduced emission reduction in fuel production and reduced costs, and contribute to system reliability. DSM options are categorized into:

- Peak shifting
- Valley filling
- Peak clipping
- Storage conservation

These options have an overall impact on the utility load curve. For distribution automation functions, DSM is classified into three categories:

1. Direct Control of Load : Uses a communication system such as a power line carrier/radio to transmit direct control of load, small generators, and storage from utility to customers.

2. Local Load Control Option: Enables customers to self-adjust loads to limit peak demand, for example, demand activated breakers, load interlocks, timers, thermostats, occupancy sensors, cogeneration heating, cooling storage, and so on.
3. Distribution Load Control: Utility controls customer loads by sending real-time prices.

3.6.5 Distribution Generation Control

More comprehensive planning approaches from the distribution system to the bulk power system are needed, including probabilistic approaches at the bulk system level. This is particularly important with the increased prevalence of distributed variable generation, for example, local wind plants and rooftop solar, on distribution systems. In aggregate, distributed variable generation needs to be treated, where appropriate, similarly to transmission-connected variable generation. The issues of note include forecasting, restoration, voltage ride through, safety, reactive power, observability, and controllability. Standard, non confidential, and nonproprietary power flow and stability models are needed to support improved planning efforts and appropriately account for new variable resources. Variable generation manufacturers are encouraged to support the development of these models.

3.7 END USER/APPLIANCE LEVEL OF THE SMART GRID

At the end-user level, significant changes in metering and monitoring are being introduced. DSM and DR are the two fundamental automation functions which will be enhanced by developments at the end-user and appliance levels. DSM includes customers as utility planning options. The total system cost including DSM cost is minimized to obtain an optimal mix of the supply side of the generation and demand side load reduction. Analysis of DSM uses techniques such as daily load curve or mathematical programming methods. DSM has been carried out using the context of unit commitment studies, optimal power flow studies, load reduction forecasting methods, engineering features of the end-user equipment interruptible load management program, survey methods (data collection), and DP to optimize energy procurement and load management by utilities.

Standards for integrating advanced mobile power recovery units, energy storage, and on-demand or peak-shaving technologies will invariably necessitate the development of standards for coordination, communication, and interoperability of multiple appliances competing for energy at the optimum grid price available. These and other related issues are research topics that require urgent attention.

3.8 APPLICATIONS FOR ADAPTIVE CONTROL AND OPTIMIZATION

There are several potential applications for adaptive controls and optimization in the development of the smart grid's design framework. It is important that adaptation and control strategy scheduling consider the stochastic and dynamically interdependent attributes of power

systems. Conventional techniques to handle these problems often suffer from the curse of dimensionality and somewhat heuristic methods which tend to give non optimal solutions. Therefore, system stochasticity and dynamic interdependence lead to unstable, non feasible and non optimal solutions.

In DSOPF, the efficient optimization technique typically based on two-stage action and critic networks are used to achieve:

- Multi objective, time-dependent optimization for complex systems
- Optimal scheduling subject to technical constraints of the plant or system
- Adaptation to perturbation of power system dynamics over time
- Adaptation to varying random noise, uncertainties, and/or missing or corrupted measurements
- Adaptation to changes in system structure while distinguishing between observable and unobservable measurements

Short and Long Answer Type Questions

1. List the barriers in implementing smart grid.
2. Enumerate in detail about the Barriers and solution to the Smart Grid.
3. Elaborate the solution pathways for Designing Smart Grid using Advanced Optimization and Control Techniques.
4. Discuss in detail about the General Level Automation of Smart Grid.
5. Describe in detail on Power System Automation on at Transmission level.
6. Explain in detail on various storage technologies used for smart grid.
7. Describe in detail on Power System Automation on at Distribution level.
8. Brief on End User/ Appliance level of the smart grid.
9. Write short notes on potential applications for adaptive controls and optimization in the development of the smart grid's design framework.

4 RENEWABLE ENERGY AND STORAGE

4.1 RENEWABLE ENERGY RESOURCES AND STORAGE

Renewable energy resources are sources of energy that can be replenished naturally, such as solar, wind, hydro, geothermal, and biomass. These sources of energy are important for reducing greenhouse gas emissions, mitigating climate change, and promoting sustainable energy production.

However, renewable energy sources have some challenges, such as their intermittent nature, meaning they are not always available when needed. This is where energy storage technologies come in. Energy storage systems store excess energy generated by renewable sources when they are available, and then release that energy when needed, helping to overcome the intermittency of renewable energy sources.

There are several energy storage technologies available today, including batteries, pumped hydro storage, compressed air energy storage, thermal energy storage, and flywheels. Battery storage, in particular, has gained popularity in recent years due to its cost-effectiveness and scalability. Lithium-ion batteries, for example, are commonly used in residential, commercial, and utility-scale energy storage systems.

In addition to storage, another way to address the intermittency of renewable energy sources is through the integration of different renewable sources. By combining solar, wind, hydro, and other renewable sources, energy production can be more predictable and reliable. Furthermore, the use of smart grid technologies can help to optimize the use of renewable energy sources and storage systems, maximizing energy efficiency and reducing energy waste.

Overall, the combination of renewable energy sources and storage technologies can help to create a more sustainable energy system, reducing greenhouse gas emissions, promoting energy independence, and creating economic opportunities in the renewable energy sector.

4.2 SUSTAINABLE ENERGY OPTIONS FOR THE SMART GRID

Sustainable energy is derived from natural sources that replenish themselves over of time. Sometimes called green power, because they are considered environmentally friendly and socially acceptable, they include sun, wind, hydro, biomass, and geo- thermal.

The future electric grid will feature rapid integration of alternative forms for energy generation as a national priority. This will require new optimization for energy resources that are distributed with interconnection standards and operational constraints. The legacy grid was designed to handle this change. The stability, reliability, and cost implications of renewable energy resources in the development of technical and economic software are vital.

Renewable energy options are meant to provide the smart grid with:

i. Remote utilization and storage of RER resources output
ii. Enhancement of functionality of grid-connected renewable energy systems (RES)
a. Facilitating give-and-take of energy from the system
b. Redistribution/reallocation of unused power from grid-connected RES
c. Facilitating storage of grid-generated and RER-generated energy by back- up storage technologies at customer end
d. Tracking interactions for billing and study
iii. Enhancement of functionality of electric vehicles and plug-in hybrids

Utilization of vehicle battery packs as energy storage devices

The common RER uses in smart grid networks are presented below.

4.2.1 Solar Energy

Solar energy harnessed by the use of photovoltaic (PV) cells was first discovered in 1839 by French physicist Edmund Becquerel. The technology can be a single panel, a string of PV panels, or a multitude of parallel strings of PV panels. Solar PV has no emissions, is reliable, and requires minimum maintenance.

The PV system generally considers:

i. Insolation: The availability of solar energy conversion to electricity. Insolation levels are affected by the operating temperature of PV cells intensity of light (location-dependent), and the position of the solar panels (maximize the power tracking while maximizing perpendicular incident light rays).

ii. Emission: PV emission levels are environmental friendly.

To improve efficiency, the materials used for manufacturing PV cells include amorphous silicon, polycrystalline silicon, cadmium telluride, microcrystalline silicon, and copper indium selenide.

4.2.2 Solar Power Technology

Solar power technology enhances PV output by concentrating a large area of sunlight into a small beam using lenses, mirrors, and tracking systems. Parabolic troughs and solar power towers are examples of such technologies.

Cost Implication: Manufacturers continue to reduce the cost of installation as new technology is developed for manufacturing materials. Much work is being conducted in the manufacturing of PV and the development of superior materials. Basic materials include monocrystalline and polycrystalline panels, cast polycrystalline silicon, and string and ribbon silicon, as well as amorphous silicon or thin film panels which are created by the application of amorphous silicon, copper indium diselenide (CIS), and cadmium telluride (CdTe) as a thin semiconductor film. This application allows for the manufacturing of panels that are less time consuming to manufacture with lower manufacturing costs and that are applicable to varied applications, albeit with reduced efficiency.

4.2.3 Modeling PV Systems

There are several PV simulation programs which allow for series analysis for time such as PV-Design Pro . The input typically consists of one year’s worth of hourly global- direct irradiance, and temperature and wind speed data, for example, TMY data, array geometry, and other PV and balance of system (BOS) parameters. Many models exist for the calculation of the power output of a PV cell or bank. Due to the varying efficiencies and numerous technologies presently available, power output is affected by environmental conditions and module specifications. The I-V characteristic model of a single cell is commonly used for PV technologies. The model is given by:

$$I = I_{sc} - I_{os}\left(e^{\frac{q(V+IR_s)}{nkT}} - 1\right) - \frac{V+IR_s}{R_{sh}}$$

$$I_{os} = AT^{\gamma} e^{\left(\frac{-E_g}{nkT}\right)}$$

$$I_d = I_{sc} - I_{os}\left(e^{\left(\frac{-q}{nkT} E_d\right)\psi} - 1\right)$$

Where for an array of $N_s \times N_{sh}$ solar cells:

$$I_d = \frac{I_{d\_\mathrm{mod}}}{N_{sh}}$$

$$E_{d\_\mathrm{mod}} = E_d \times N_s$$

$$R_{s\_\mathrm{mod}} = R_s\left(\frac{N_s}{N_{sh}}\right)$$

$$R_{sh\_\mathrm{mod}} = R_{sh}\left(\frac{N_s}{N_{sh}}\right)$$

Where

I: current flowing into load of a solar cell (A) I_{sc}: short circuit current (A)

I_{os}: saturation current (A) s: insolation (kW/m^2)

q: electron charge (1.6 x 10^{-19} (C))

k: Boltzmann constant (1.38 x 10^{-23} (JK^{-1})) T: p-n junction temperature (K), t (^{o}C)

N: junction constant

A: temperature constant

γ: temperature dependency exponent E_g: energy gap (eV)

V: voltage across solar cell (V)

V_{oc}: open circuit voltage of a solar cell (V)

R_s, R_{s_mod}: series parasitic resistance for cell and entire module (Ω)

R_{sh}, R_{sh_mod}: shunt parasitic resistance for cell and entire module (Ω)

E_d, E_{d_mod}: across voltage of an ideal solar cell and entire module (V)

I_d, I_{d_mod}: current of an ideal solar cell and entire module (A)

N_s: number of series cell junctions of a PV module

N_{sh}: number of parallel cell junctions of a PV module

V_{out}: across voltage of a PV module (V)

I_{out}: current of a PV module (A) R: connected load (Ω)

An alternative equation for the modeling of the output of the PV panels is [6]:

$$P_{mp} = \frac{G}{G_{ref}} P_{mp,ref} \left[1+\gamma \left(T - T_{ref}\right)\right]$$

where

G is the incident irradiance

P_{mp} is the maximum power output

$P_{mp,ref}$ is the maximum power output under standard testing conditions T is the temperature

T_{ref} is the temperature for standard testing conditions reference (25°C)

G_{ref} = 1000 Wm−2

γ is the maximum power correction for temperature

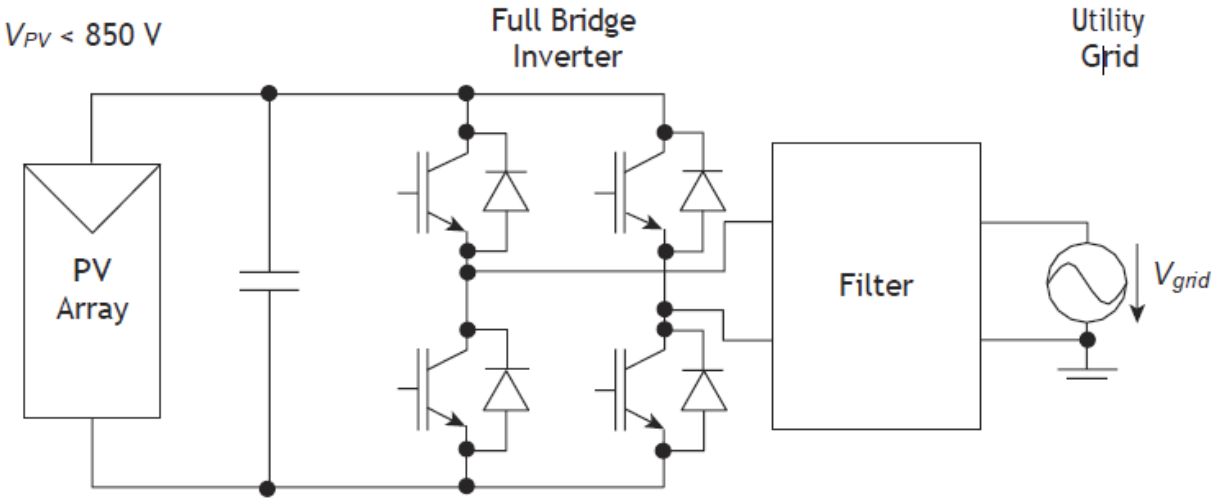


Figure 4.1 PV inverter system for DC-AC conversion

The PV output is variable due to in relation to the solar insolation and surface temperature. The data for predicting the solar input is several years of measurements of irradiance on the proposed locator. These statistical measures may be estimated from meteorological data available from the site, from a nearby site having similar irradiance, or from

an official solar atlas or database. Solar insolation has been modeled probabilistically for variability studies of PV systems utilizing various distributions including Gaussian (normal) and Beta probability density functions.

Conversion and Power Electronic Technology. Several inverter systems convert or transform the DC into AC for grid-connected PV systems (see Fig. 4.1).

Penetration of PV into the smart grid requires studies in variability and conversion technology. The mathematical models and probability density used to model PV behavior include Beta and Rayleigh density functions. The tracking method based on fuzzy/ GA technologies is able to obtain enough power points for effective delivery. Siting and sizing of PV uses classical and computational intelligence methods that involve decisions based on real-time data.

4.2.4 Wind Turbine Systems

Wind is one of the fastest-growing sources of renewable energy throughout the world (see Fig. 4.2). Turbines produce electricity at affordable cost without additional investments in infrastructure such as transmission lines. A wind turbine consists of a rotor, generator, blades, and a driver or coupling device. Compared with PV, wind is the most economically competitive renewable.

Both wind speed and the height of pole-mounted units contribute to the power output. Although turbines produce no CO_2 or pollutants, wind has three drawbacks: output cannot be controlled, wind farms are most suited for peaking applications, and power is produced only when there is sufficient wind

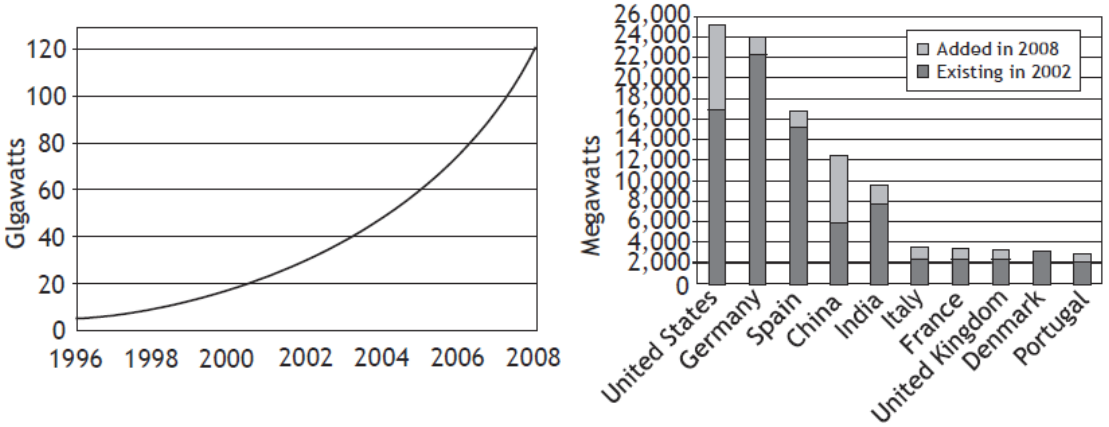


Figure 4.2. (a) Wind power, existing world capacity, 1996-2008; (b) Wind power capacity, top ten countries, 2008

Modeling Wind Turbines: Machines which consume reactive power and produce real power. The quantification of the capacity/real power output is given by:

$$P_m = \frac{1}{2}\rho \cdot \pi R^2 \cdot V^3 \cdot C_p$$

ρ is the air density (kg/m^3)

R is the turbine radius (m)

Cp is the turbine power coefficient power conversion efficiency of a wind turbine

V is the wind speed (m/s)

The electrical power output is given by:

$$P_e = n_o P_m$$

Where

$n_o = \eta_m \eta_g$

η_m, and η_g are the efficiency of the turbine and the generator, respectively

Wind energy options are typically random and require a modeling technique based on probability such as Gaussian, Rayleigh, and Beta pdfs. Another challenge is congestion management. Due to time varying behavior and randomness, EP such as GA, ANN, and fuzzy logic and its hybrids are used to allocate wind energy to meet in-time local demand. The process includes obtaining real-time measurement, and using the system state, location, and network limitation to define new algorithms.

4.2.5 Biomass-Bioenergy

Bioenergy is the energy derived from organic matter such as corn, wheat, soybeans, wood, and residues that can produce chemicals and materials. Biopower is obtained from a process called gasification, converting gas to gas turbines to generate electricity. Biomass can be converted directly into fluid fuels such as ethanol, alcohol or biodiesel derived from corn ethanol.

Biomass plants are commercially available in the United States for up to 11GW of installed capacity. Biomass power ranges from 0.5 GW to 3.0 GW using landfill gas and forest products, respectively. Biomass has traditionally been used for domestic cooking and heating in developing countries. It can produce power only when sufficient bioproducts are available and the conversion process is undertaken. Biomass produces CO_2 and other emissions. The desirable scheduling and allocation strategy for biomass in real time requires the capability to include variability of the modeling using new system theory concepts.

4.2.6 Small and Micro Hydropower

Hydropower is by far the largest renewable source of power/energy. Small hydro- power systems vary from 100 kW to 30 MW while micro hydropower plants are smaller than 100 kW. Small hydropower generators work in variable speed because of water flow. Induction motors provide a generator for a turbine system. The hydraulic turbine converts the water energy to mechanical rotational energy.

Small and micro hydropower systems are RER optimizations to enhance the smart grid. The issues of reliability and modeling are addressed as in PV and wind energy. CI technology is used for performance study and commitment

4.2.7 Fuel Cell

Fuel cells can also be used to enhance power delivery in the smart grid. They are simply fuels from hydrogen, natural gas, methanol, and gasoline. The efficiency for fuel to electricity can be high as 65% since it does not depend on Carnot limits. Fuel cells are environmentally friendly by efficient use of fuel. Different forms include phosphoric acid (PAFC), proton exchange membrane (PEM), solid polymer molten carbonate (MCFC), solid oxide (SOFC), alkaline (a direct methanol), regenerative fuel cells, and botanic ceramic fuel cells (PCFC). Fuel cells produce virtually no emissions. Their cost is significantly high compared with conventional technologies

The topology of a fuel cell is a stack which consists of the part of the fuel cell that holds the electrodes and electrolytic material. Hydrogen is extracted from gasoline propane, with natural gas refineries to operate fuel cells commercially. Emission is very low and so these cells have minimum environmental impacts. The high efficiency leads to low fuel costs and minimum maintenance due to lack of moving parts. They have virtually no pollutant emission as CO_2 is rather low. They are a good fit for green power and premium power due to their quality. In addition, they provide a moderate high thermal quantity output and hence are ideal for CHP. However, they perform poorly as peaking power due to extremely high capital costs.

The efficiency of fuel cells ranges from 40–80%. Two commonly used fuel cell types are phosphoric acid fuel cells (PAFC), which operate at relatively high temperatures and use an external water cooling system to cool the stack, and proton exchange membrane fuel cells, which operate at a lower temperature than most other fuel cells and contain no chemicals such as liquid acids or molten bases that would cause concerns about materials of construction.

4.2.8 Geothermal Heat Pumps

This form of power is based on accessing the underground steam or hot water from wells drilled several miles into the earth. Conversion occurs by pumping hot water to drive conventional steam turbines which drive the electrical generator that produces the power. The water is then recycled back into earth to recharge the reservoir for a continuous energy cycle. There are several types of geothermal power plants including dry steam, flash stream, and binary cycle. Dry steam plants draw water from the reservoirs of steam, while both flash steam and binary cycle plants draw their energy from the recycled hot water reservoir.

In the United States, geothermal power is produced in California, Utah, Nevada, and Hawaii. Various applications of geothermal power include heat pumps, agriculture, fishing, farming, and food processing. Geothermal projects require significant upfront capital investment for exploration, drilling wells, and equipment. Exploration risk and environmental impacts are considered in geothermal power plant projects

4.3 PENETRATION AND VARIABILITY ISSUES ASSOCIATED WITH SUSTAINABLE ENERGY TECHNOLOGY

The degree of penetration by sustainable energy into today's grid varies by location, depending on the availability of the conditions necessary for viable utility. This can be quantified by:

$$\text{Penetration Level} = \frac{\sum_{\forall i} P_{DG,i}}{\sum_{\forall j} P_{demand,j}}$$

The selection and implementation of the available sustainable energy technologies are subject to the issues of variability associated with the sources, for example, solar and wind. For solar energy, the variation of the solar radiation is a function of the time, location, height above the earth's surface, local weather conditions, and degrees of shading. The variability of the PV source is a function of the solar insolation which has been modeled using a Beta distribution function. Utilizing historical data for location and time allows calculation of parameters of the Beta model by solving equations given as

$$\alpha = \mu\left(\frac{(1-\mu)\mu}{\sigma} - 1\right)$$

$$\beta = (1-\mu)\left(\frac{(1-\mu)\mu}{\sigma} - 1\right)$$

The corresponding probability distribution function is formulated as *f*(*s*):

$$f(s_i) = \frac{s_i^{\alpha-1}(1-s_i)^{\beta-1}}{\Gamma(\alpha)\Gamma(\beta)}\Gamma(\alpha+\beta)$$

There are three apparent sources of variability in wind technology: wind speed random variability, turning off turbines to prevent damage when wind speed values are greater than the tolerable limit and no output when wind speed is less than the cut-in speed. The Weibull model, which has been used for studying wind speeds since 1978, models wind speed trends in numerous instances. The probability density function is:

$$f(V) = \begin{cases} \frac{k}{\lambda}\left(\frac{V}{\lambda}\right)^{k-1} \exp\left(\frac{V}{\lambda}\right)^{k}, V \geq 0 \\ 0, V < 0 \end{cases}$$

with mean and variance calculated in terms of the shape and scale parameters

$$\mu = \lambda\Gamma\left(1+\frac{1}{k}\right)$$

$$Var = \lambda^2\Gamma\left(1+\frac{2}{k}\right) - \mu^2$$

Utilizing historical data for location and time, the parameters of the Weibull model can be determined by simultaneously solving the mean and variance equations given as

$$k = \left(\frac{\sigma}{\bar{V}}\right)^{-1.086}$$

$$\lambda = \frac{\bar{V}}{\Gamma\left(1+\left(\frac{1}{k}\right)\right)}$$

Another common model is the Rayleigh distribution function, a special case of the Weibull model, which offers the added simplicity of only one parameter. This assumption can be made in several instances where the wind scale parameter in the location under study is approximately.

The concept of smoothing mitigates the impact of variability by utilizing several turbines over an area. From this penetration level an optimal scheme based on the computational intelligence technique is proposed for evaluating system and stability assessment in real time.

4.4 DEMAND RESPONSE ISSUES

Energy management involves controlling electrical and mechanical systems to reduce power needs and the associated costs. DR helps to reduce customer demand on the grid that is dependent on that demand. Abundant data, including price signals and grid conditions, allow

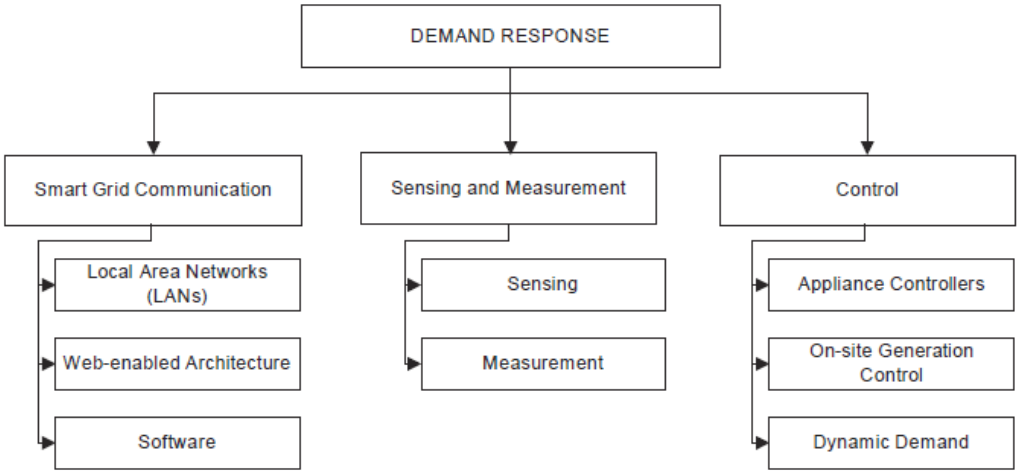


Figure 4.3. Demand Response technology tree

DR technologies to play a significant role. Monitoring operating parameters such as voltage, angle, and frequency of the system are utilized through real-time sensors in addition to controllers, metering signals, and two-way digital communication, in responding to changes in the grid and electricity prices. Automatic DR in times of disruption is a key feature of the smart grid, as are smart meters, smart appliances, and distributed RER. To achieve optimal control of demand and fulfill economic and environmental goals, utilities can show customers how to adjust their consumption to off-peak time demand to assist in efficient supply.

Figure 4.3 shows the DR applications that can be categorized into four components:

A. Energy Efficiency
B. Price-based DR
    a. Time-of-use (TOU)
    b. Day-ahead hourly pricing
C. Incentive-based DR
    a. Capacity/ancillary services

b. Demand bidding buy-back
c. Direct load control

D. Time scale commitments and dispatch
a. Years of system planning
b. Months of operational planning
c. Day-ahead economic scheduling
d. Day-of economic dispatch
e. Minutes dispatch

4.5 ELECTRIC VEHICLES AND PLUG-IN HYBRIDS

The integration of electric vehicles and hybrids is another component of the smart grid system. Vehicle-to-grid power (V2G) uses electric-drive vehicles (battery, fuel cell, or hybrid) to provide power for specific electric markets. V2G can provide storage for renewable energy generation and stabilize large-scale wind generation via regulation. Plug-in hybrids can dramatically cut local air pollution. Hybridization of electric vehicles and connections to the grid overcome limitations of their use including cost, battery size/weight, and short range of application. PHEVs provide the means to replace the use of petroleum-based energy sources with a mix of energy resources (encountered in typical electric power systems) and to reduce overall emissions.

PHEVs offer advantages and disadvantages compared to other proposed solutions. The deployment of PHEVs potentially has a substantial positive impact on the electric power system from the point of view of increasing electric energy consumption, offset- ting petroleum fuels with alternative sources of energy.

4.6 PHEV TECHNOLOGY

Through V2G power, a parked vehicle can provide power to the grid as a battery- electric, fuel-cell, or even a plug-in hybrid vehicle. Stored or unused energy that utilities reserve at night or during off-peak times can be used to support the vehicles in cases of extreme emergencies, for example, a significant decrease in oil supplies or a sudden rise in oil prices. It should be noted that electric drive systems are considered 70% efficient, for example, a first-generation plug-in hybrid can travel approximately 3–4 miles per kWh, or about 75 cents per gallon of gas.

Each PHEV vehicle will be equipped with a connection to the grid for electrical energy flow, a control or logical connection necessary for communication with the grid operator, and onboard controls and metering. Figure 4.4 schematically illustrates the connections between vehicles and

the grid. Electricity flows through- out the grid from generators to end-users while unused energy flow backs from the EDVs as shown by the lines with two arrows in Figure 4.4 Note that during times of low demand, battery EDVs can charge and discharge as necessary for power supply or demand. Fuel cells can create power from liquid and gaseous fuels and plug-in hybrids can function in either capacity.

4.6.1 Impact of PHEV on the Grid

PHEVs are expected to take 10% of the U.S. market share of new vehicles sold in 2015, and 50% of the market share by 2025. Utilities have become concerned with the number of PHEVs coming on the market because there may be insufficient supply for the increased demand resulting from additional load for battery charging.

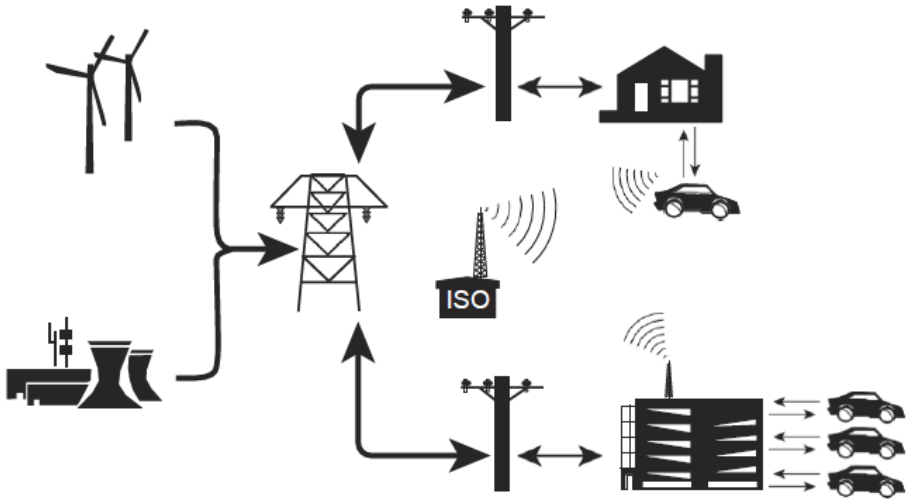


Figure 4.4. Schematic of proposed power line and wireless control connections between electric vehicles and the grid

By 2040, the addition of PHEV battery charging in the United States will increase existing load by 18%. Unfortunately, this increase in load will eventually cause voltage collapse in amounts up to 96% of the nominal voltage in some areas, requiring the integration of transformers, capacitors, and other power distribution devices for mitigation.

It will be critical to study the trends of daily PHEV power usage and the average power consumption over one day to determine the impacts on the grid, market, environment, and economy. Peak driving levels will coincide with existing early and end-of- day peaking hours when users are waking up and heading to work and when they are home, having supper, and so on. During peak hours the increased need for energy may require users to charge their PHEVs in high-peak hours. Regulation of charge times will help maintain stability throughout the network.

4.7 ENVIRONMENTAL IMPLICATIONS

Environmental impact mitigation is a major driver of smart grid development. The integration/facilitation of the use of renewable energy resources for generation and the move towards the use of PHEVs are two critical aspects of the environmental implications of the smart grid. In addition the increased energy efficiency, demand response and load management will result in a stable development of clean power market.

4.7.1 Climate Change

Climate change is the term commonly linked to the issue of global warming and cooling resulting from the increased emissions of greenhouse gases (GHG). The term climate change refers to any distinct change in measures of climate lasting for a long period of time, that is, major changes in temperature, rainfall, snow, or wind patterns lasting for decades or longer.

Climate change may result from:

- Natural factors, such as changes in the Sun's energy or slow changes in the Earth's orbit around the Sun.
- Natural processes within the climate system, for example, changes in ocean circulation
- Human activities that change the atmosphere's composition (for example, burning fossil fuels) and the land surface (for example, cutting down forests, planting trees, and expanding cities and suburbs)

Global warming is an average increase in temperatures near the Earth's surface and in the lowest layer of the atmosphere. Increases in temperatures in the Earth's atmosphere can contribute to changes in global climate patterns. Global warming can be considered part of climate change along with changes in precipitation, sea level, and so on.

Global change is a broad term that refers to changes in the global environment, including climate change, ozone depletion, and land use change.

4.7.2 Implications of Climate Change

The key implications of climate change include:

- Energy: Increased temperatures will cause an increase in energy bills as consumers use more air conditioning.
- Health: Extremes of temperature such as excessive and long-term exposure to heat will contribute to disease.
- Agriculture and Wildlife: Irregular weather variability implies lack of proper water supply, and increased temperature may result in worsening crop production and, ultimately, rising food costs.

- Water Resources: Temperature and weather irregularity increase the possibility of flooding and droughts and impact the quality and availability of global fresh water supply. As the water supply is affected, farmers will need to irrigate crops.

The DOE's strategic plan for a U.S. Climate Change technology program involves:

- The facilitation of DG, particularly RER technology
- The development of energy storage technology to conserve generated energy
- The advancement of DR to decrease demand

Consumer education and participation should increase sensitivity to the issues. Discussion of the potential contribution of RER on climate change will consider the projected increase, from the current 13% to 30%, as well as the following improvements to the grid:

i. Improvement from 5% to 15% in DR systems
ii. Improvement from 1% to 10% in consumer generation
iii. Improvement from 47% to 90% of asset utilization
iv. Improvement in transmission asset utilization from 50% to 80%
v. Improvement in distribution asset utilization from 30% to 80%

4.8 ENERGY STORAGE TECHNOLOGIES

Energy storage is important for utility load leveling, electrical vehicles, solar energy systems, uninterrupted power supply, and energy systems in remote locations. Energy storage has always been closely associated with solar installations, including solar heating and PV. Storage options are particularly essential when variable sources are used in islanding and standalone power systems. Figure 4.5 presents a sample topology for a microgrid system.

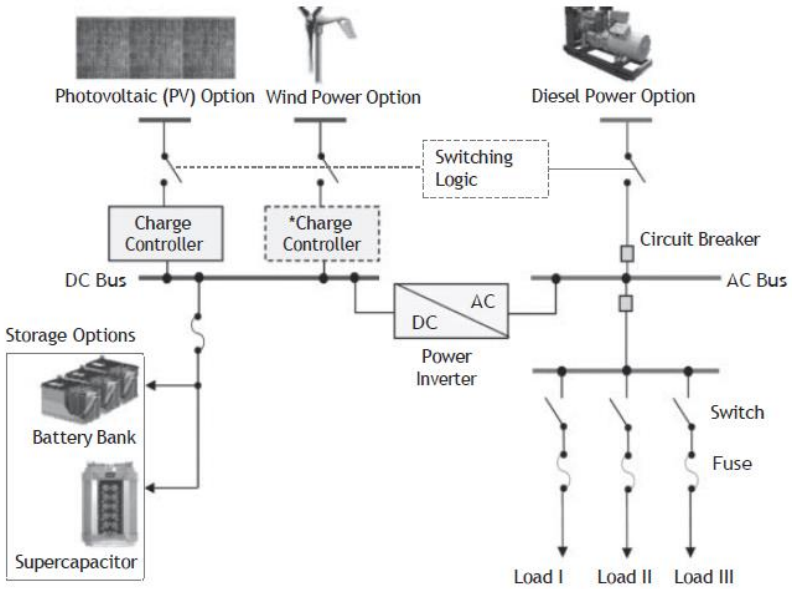


Figure 4.5. Microgrid topology with storage technologies

There are two principal reasons why energy storage will grow in importance with the increased development of RER:

1. Many important RER are intermittent, generating when the weather dictates, rather than when energy demand dictates.
2. Many transportation systems require energy to be carried with the vehicle.

Storage options can be evaluated based on the characteristic of the application, for example, whether the application requires portable or fixed storage methods, the duration when storage will be operational, and the maximum power needed for the application. The selection of the proper storage technology is based on the following parameters:

- **Unit Size**: Scale of technology. Storage technologies have an associated range for application, for example, large units support grid-connected RER technologies.
- **Storage Capacity**: Total store of available energy after charging.
- **Available Capacity**: Average value of power output based on the state of charge/ depth of discharge.
- **Self-discharge Time**: Time required for a fully charged, non-interconnected storage device to reach a certain depth of discharge (DOD), this is contingent on the operational condition of the system.
- **Efficiency**: Ratio of energy output from the device to the energy input issue of conversion technology and design of RER and storage and conversion needed.
- **Durability or Life-cycle**: Number of consecutive charge-discharge cycles a storage installation can undergo while maintaining the installations and other specifications within limited ranges. Life-cycle specifications are made against a chosen DOD depending on the applications of the storage device.
- **Autonomy:** Ratio between energy capacity and maximum discharge power; indicates the maximum amount of time the system can continuously release energy.
- **Mass and Volume Densities:** Amount of energy accumulated per unit mass or volume of the storage unit.
- **Cost:** Cost of installation, operation, and maintenance of storage technology; cost should be analyzed throughout system lifespan.
- **Feasibility:** Degree of adaptability to the storage applications.
- **Reliability:** Guarantee of service.

Additional information characteristics include monitoring and control equipment, operational constraints, environmental impacts, ease of maintenance, simplicity of design, operational flexibility, and response time for energy release.

4.9 TYPES OF ENERGY STORAGE TECHNOLOGIES

4.9.1 Batteries

Batteries store energy in chemical form during charging and discharge electrical energy when connected to a load. In its simplest form a battery consists of two electrodes, a positive and a negative placed in an electrolyte. The electrodes exchange ions with the electrolyte and electrons with the external circuit.

Lead acid and Sodium Sulfur (NaS) batteries are used at present for large utility applications in comparable numbers. Lithium Ion (Li-ion), Nickel Cadmium (NiCd) and Nickel metal hydrides (NiMH) are also thought to be promising future options.
Lead acid batteries have been used for many years in utility applications, providing excitation for synchronous machines and acting as back-up auxiliary power supplies. They are cheap but need significant maintenance. Their lifetime is comparatively short particularly if discharged deeply.

NaS batteries operate at 300–400 ◦ C and have a large energy capacity per unit volume and weight. They are used for electrical energy time shifting (for example, Citizens Substation, USA, 2 MW (Figure 4.4), 12 MWh), wind farm support (for example, East Busco Substation, USA, 1MW, 6 MWh) and to smooth the output of PV generators.

Figure 4.6 is a simplified drawing of a NaS battery. The positive electrode is molten sulfur and the negative electrode is molten sodium. The electrolyte, which is a sodium beta-alumina ceramic (four layers of oxygen atoms and aluminium in the same atomic arrangement), allows ion exchange to take place. More details about the operation of a NaS battery are given in [3].
Li-ion is gaining its place as a distributed energy storage system, in particular with the developing use of Li-ion batteries in electric vehicles. These have a graphite negative electrode and lithium cobalt oxide, lithium iron phosphate or lithium manganese oxide positive electrode. The electrolytes generally use lithium salt in an organic solvent.

NiCd batteries were extensively used for power tools, mobile phones and laptops. However, this material has effectively been displaced from these markets by other batteries over the past decade. The robust nature of the technology, combined with its energy density, gives it

advantages over lead acid and led to NiCd being chosen for the flagship battery energy storage project in Golden Valley in Alaska.

Figure 4.6 Rock County Substation, Beaver Creek, Minnesota: 1 MW, 6 MWh NaS battery- based storage system installed at the point of interconnection of the Minwind 12 MW wind farm. Source: Courtesy of S & C Electric Europe Ltd.

4.9.2 Flow battery

A flow battery uses two electrolytes, often different kinds of the same chemical compound. Both the positive and negative electrolytes are stored separately and are pumped through a cell. Inside the cell, the two electrolytes are kept separate. The electrochemical reaction takes place by transferring ions across a membrane as shown in Figure 4.7. The electrodes do not take part in the chemical reaction and thus do not deteriorate from repeated cycling (one of the problems in other types of batteries that leads to loss of performance over time).

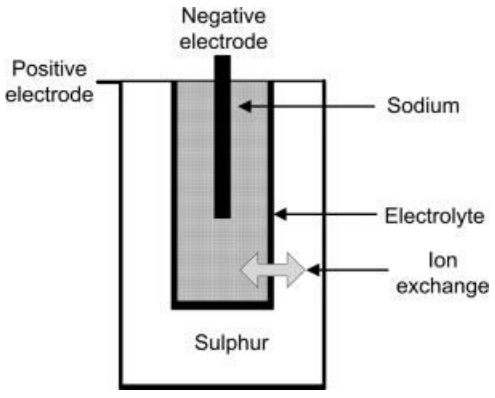


Figure 4.7 A NaS battery

The amount of energy stored in a flow battery depends on the volume of the electrolyte in the tanks whereas the power output depends on the speed of ion transfer across the membrane. Flow batteries using Zinc Bromide (ZBB) and Vanadium Redox (VRB) are available. A ZBB consists

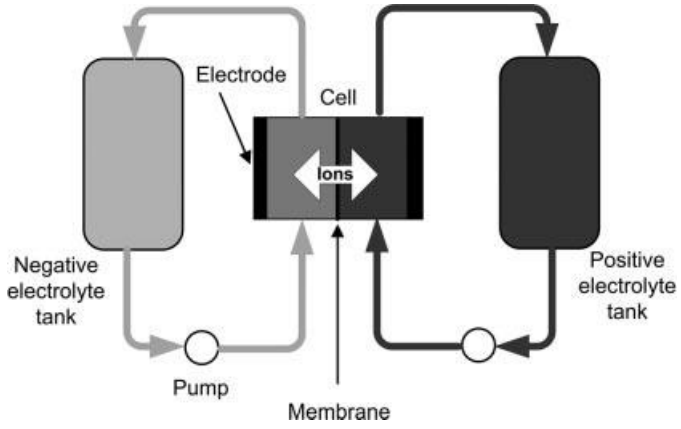


Figure 4.8 Construction of a flow battery

of a zinc negative electrode and a bromine positive electrode separated by a micro-porous membrane. An aqueous solution of zinc bromide (ZnBr) is circulated through the two compartments of the cell from two separate reservoirs as shown in Figure 4.8. On discharge, the zinc is oxidised, giving zinc ions, and the bromine is reduced to bromide ions. During charging, zinc is electroplated on the negative electrode and bromine is evolved at the positive electrode; this is stored as a chemically complex organic phase at the bottom of the positive electrolyte tank. A third pump is used for recirculation of the organic phase during the discharge cycle.

The reactions that occur at the two electrodes during charge and discharge are:

$$\text{Positive electrode: } Br_2(aq) + 2e^- \underset{\text{Charge}}{\overset{\text{Discharge}}{\rightleftharpoons}} 2Br^-$$

$$\text{Negative electrode: } Zn \underset{\text{Charge}}{\overset{\text{Discharge}}{\rightleftharpoons}} Zn^{2+} + 2e^-$$

In VRB, V2 /V3 and V4 /V5 redox couples in sulphuric acid are stored in electrolytic tanks with an ion exchange membrane. The reactions that occur in the battery during charging and discharging are:

$$\text{Positive electrode: } V^{5+} + e^- \underset{\text{Charge}}{\overset{\text{Discharge}}{\rightleftharpoons}} V^{4+}$$

$$\text{Negative electrode: } V^{2+} \underset{\text{Charge}}{\overset{\text{Discharge}}{\rightleftharpoons}} V^{3+} + e^-$$

There have been a number of demonstration projects with flow batteries of capacities ranging from a few kW to several MW with storage up to 10 hours at full output.

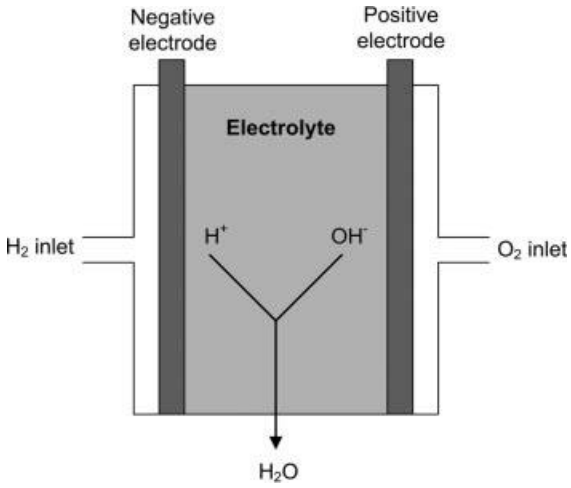


Figure 4.9 Simplified diagram of a fuel cell

4.9.3 Fuel cell and hydrogen electrolyser

Most fuel cells use H2 and O2 as their main fuel (Figure 4.9). At the negative electrode, hydrogen is oxidised to form H+ and electrons. The electrons flow through the external electrical circuit whereas the hydrogen ions move towards the positive electrode through the electrolyte. The positive electrode is made from a porous material coated with a catalyst. At that electrode, the hydrogen ions combine with oxygen to produce water.

Many different types of fuel cells have been developed and their characteristics are listed in Table 4.1.

Table 4.1 Different types of fuel cells

Type	Electrolyte	Operating temperature	Maximum output power reported
Polymer Electrolyte Membrane (PEM)	Organic polymer	80 °C	250 kW
Alkaline Fuel Cells (AFC)	Potassium hydroxide	150–200 °C	12 kW
Phosphoric Acid Fuel Cell (PAFC)	Phosphoric acid	150–200 °C	250 kW
Molten Carbonate Fuel Cells (MCFC)	Potassium, sodium or lithium carbonate	650 °C	2 MW
Solid Oxide Fuel Cells (SOFC)	Ceramic materials	1000 °C	100 kW

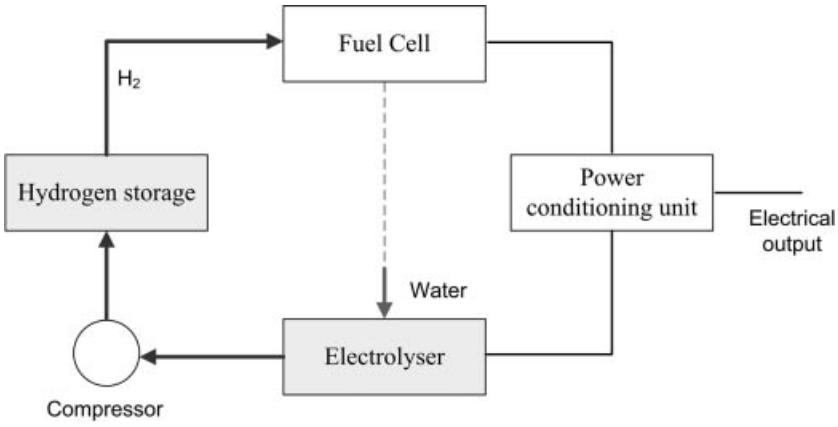


Figure 4.10 Hydrogen energy storage systems

Hydrogen-based energy storage systems consist of an electrolyser, hydrogen storage and a fuel cell, as shown in Figure 4.10. The electrolyser uses electrical energy to produce H2 from water. One of the potential applications of this device is to store H2 when there is excess wind energy generation and then use the stored H2 to support the power system during peak demand periods. Regenerative fuel cells which consume electricity and act as an electrolyser (to produce H2) have also been developed.

4.9.4 Flywheels

Flywheels store kinetic energy in a rotating mass and release it by slowing the rotation when electrical energy is required. Their application to date has mainly been for power quality and to provide energy for UPS. The majority of installations are on customers' premises with a very few applications in demonstration micro-grids.

Consider the simple rotating disc shown in Figure 4.11. The stored energy is proportional to the square of the rotor speed (ω) and the moment of inertia of the rotating mass (J):

$$\text{Storedenergy} = \frac{1}{2}J\omega^2 \tag{4.1}$$

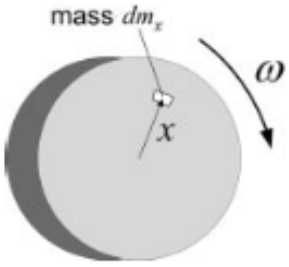


Figure 4.11 A rotating disc

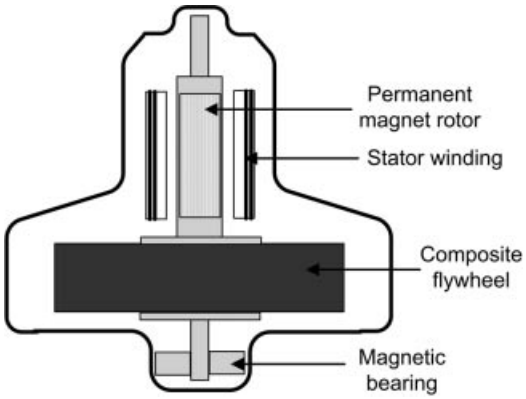


Figure 4.12 Cross- section of flywheel

The moment of inertia is given by :

$$J = \int x^2 \times dm_x \tag{4.2}$$

where *x* is the distance to an element of mass *dmx* from the axis of rotation.

From Equation (4.1), it is clear that to store energy, two options can be used: a low speed flywheel which uses a heavy steel rotor with high inertia or a high speed flywheel which uses lighter composite materials.

As given in Equation (4.2), the location of the mass is important. In some designs the mass is formed as a rim, placed away from the axis of rotation, to maximise the moment of inertia. High speed flywheels, which rotate at up to 50,000 rpm, operate in a vacuum with mag- netic bearings in order to reduce friction losses. A cross-section of a flywheel is shown in Figure 4.12.

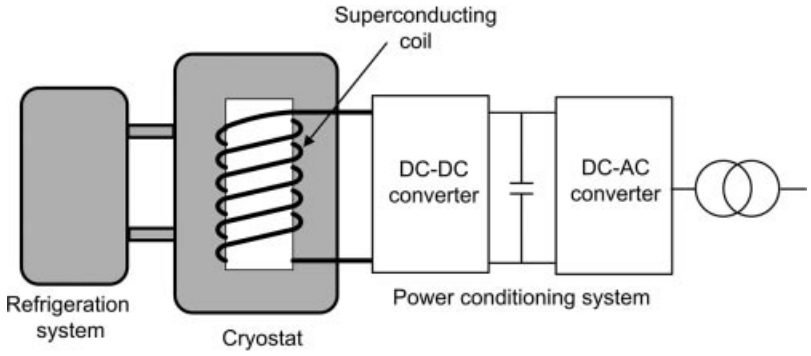


Figure 4.13 Component of superconducting energy storage

4.9.5 Superconducting magnetic energy storage systems

In a SMES system, a magnetic field is created by direct current passing through a superconducting coil (Figure 4.13). In a superconducting coil, resistive losses are negligible and so the energy stored in the magnetic field (equal to $LI2$ 2 where L is the inductance of the coil and I is the current passing through the coil) does not reduce with time. However, in order to maintain the superconductivity of the SMES coil, a cryostat which can keep the temperature of the coil below the superconductor temperature limit is required. The optimum operating temperature of high temperature superconductors, that are favoured for energy storage appli- cations, is around 50–70 K. Further, as the magnetic field produced by a SMES is large, a strong supporting structure is needed to contain the electromagnetic forces. The stored energy in the SMES is retrieved when required by a power conditioning system that is connected to the AC network as shown in Figure 4.13.

4.9.6 Supercapacitors

In a capacitor, energy is stored in an electrostatic field. The quantity of energy stored, E, is given by:

$$E = \frac{1}{2}CV^2$$

where C is the capacitance and V is the voltage across the capacitor. In a parallel plate capacitor

$$C = \frac{\varepsilon_r \varepsilon_o A}{d}$$

where εr is the relative permittivity of the dielectric material, εo is the permittivity of free space, A is the surface area of the plates and d is the distance between two plates.

Super capacitors have a double layer structure that uses a porous electrolyte such as Polyethylene Terephathalate (PET). The double layer structure increases energy storage capability significantly due to a large increase in surface area, thus C. Further, the higher relative permittivity of PET (about 3.5 at 20 ◦ C) compared to the electrolytes used in thin film capacitors also contributes to the increase in stored energy. Super capacitors are constructed with a carbonised porous material as one electrode and a liquid chemical conductor as the other electrode.

4.10 TAX CREDITS

Tax credits are examples of incentives to promote customer buy-in and participation in the utilization of RER and practice of energy efficiency. The DOE offers a number of tax credits to consumers. These include:

- Home Energy Efficiency Improvement Tax Credit: Consumers who purchase and install specific products, such as energy-efficient windows, insulation, doors, roofs, and heating and cooling equipment in existing homes can receive a tax credit for 30% of the cost, up to $1,500.
- Residential Renewable Energy Tax Credit: Consumers who install solar energy systems (including solar water heating and solar electric systems), small wind systems, geothermal heat pumps, and residential fuel cell and micro turbine systems can receive a 30% tax credit.
- Automobile Tax Credit for Hybrid Gas-Electric and Alternative Fuel Vehicles: Individuals or businesses that buy or lease a new hybrid gas-electric car or truck are eligible. Hybrid vehicles that use less gasoline than the average vehicle of similar weight and that meet an emissions standard qualify for the credit. Alternative-fuel vehicles, diesel vehicles with advanced lean-burn technologies, and fuel-cell vehicles are also eligible for tax credits.
- Automobile Tax Credit for Plug-In Electric Vehicles: The minimum amount of the credit is $2,500 and the credit tops out at $7,500, depending on the battery capacity.
- Automobile Tax Credit for Plug-In Hybrid Conversion Kits: The credit is equal to 10% of the cost of converting a vehicle to a qualified plug-in electric drive motor vehicle. The maximum amount of the credit is $4,000.
- Automobile Tax Credit for Low Speed & 2- or 3-Wheeled Vehicles: The Federal Recovery Act creates a special tax credit for certain low-speed electric vehicles and 2- or 3-wheeled vehicles. The amount of the credit is 10% of the cost of the vehicle, up to a maximum credit of $2,500.

Short and Long Answer Type Questions

1. Discuss the sustainable energy options for the smart grid in detail.
2. Analyze on the modeling of PV System in detail.
3. Describe the penetration and variability issues associated with sustainable energy technology.
4. Explain in detail about Demand Response technology tree.
5. Analyze the Plug in Hybrid Electric Vehicles (PEHV) technology for Smart Grid in a Power System Network.
6. Brief on the impact of PHEV on the grid.
7. Explain the environmental impact on implementing the smart grid.
8. Discuss the Storage Technologies used in Smart Grid.
9. Write short notes on Tax credits.

5 INTEROPERABILITY, STANDARDS AND CYBER SECURITY

5.1 INTRODUCTION

Interoperability, standards, and cyber security are essential components of the smart grid environment. These components ensure that the various components of the smart grid can work together seamlessly, that data is collected and communicated accurately and securely, and that the smart grid is protected against cyber threats.

Interoperability refers to the ability of different systems and devices to communicate and exchange data with each other. In the smart grid environment, interoperability is essential to ensure that smart meters, sensors, control systems, and other components can work together to deliver a more efficient and reliable power system.

Standards are also important for ensuring interoperability and consistency across different systems and components of the smart grid. Standards such as the IEEE 2030.5 and IEC 61850 provide guidelines for the design, installation, and operation of smart grid systems and components, ensuring that they work together effectively and efficiently.

Cyber security is also critical for the smart grid environment. The smart grid relies on advanced digital communication networks, making it vulnerable to cyber threats such as hacking, malware, and other malicious attacks. Cybersecurity measures such as encryption, firewalls, and intrusion detection systems are essential to protect the smart grid against these threats and ensure the privacy and security of sensitive data.

In addition to technical measures, policies and regulations also play a crucial role in ensuring cybersecurity in the smart grid environment. Governments and regulatory bodies may establish rules and standards for cybersecurity practices, and utilities and energy companies may develop cybersecurity policies and procedures to protect their systems and data.

Overall, interoperability, standards, and cybersecurity are essential components of the smart grid environment, enabling a more efficient, reliable, and secure power system that can meet the changing needs of consumers and the demands of the 21st-century energy landscape.

5.2 INTEROPERABILITY

Interoperability is "the ability of two or more systems or components to exchange information and to use the information that has been exchanged." The issues include the interoperation of system components supposedly conforming to a particular standard as well as the interoperation of components across standards. Merely having complete compliance to applicable smart grid standards is not enough to ensure interoperability. For example, the International Electro technical Commission (IEC) identifies the various objects and attributes as mandatory, optional, or conditional. Communications, management, security, and application execution messages must all be well understood by the interoperating equipment. A careful approach will include:

- Reviewing the activities of governing bodies: The outcome will determine the activities to be undertaken by smart grid users
- Reviewing components before deployment: Ensure compatibility with functional requirements
- Developing internal project standards: Address continuing issues and the govern- ing body efforts

5.2.1 State-of-the-Art-Interoperability

Interoperability is a key assumption in the development of smart metering to facilitate the competitive energy retail market. There are two elements to interoperability: technical and commercial. Technical interoperability is largely about defining the functionality for gas and electricity metering interfaces providing smart metering (format and data content) service requirements. The definition of technical interoperability will depend on the market model the use of smart metering.

WAN and LAN communications interfaces will be explored. Consumer engagement essential to delivering consumer benefits will be identified in a cost benefit analysis. Use of case studies will have to be forward looking to ensure that opportunities such as DSM and smart grids are not precluded by any solution.

5.2.2 Benefits and Challenges of Interoperability

Interoperability allows a network to seamlessly and autonomously integrate all components of electric power supply, particularly monitoring and measurement equipment, distribution and substation equipment, and management and communication equipment. The minimization of human intervention in this process is an important benefit of this functionality

The challenges include the need for technical enhancement of the network, adoption and adaptation of existing technologies, and development and implementation of comprehensive standards. Procedures to address vandalism, hacking, and malicious attacks will require the development of security protocols for authentication and validation before access is granted

5.2.3 Model for Interoperability in the Smart Grid Environment

Several key features in the interoperable efficiency of a network have to be considered in relation to each other and also independently. The following illustrates a conceptual model of the smart grid developed by the Grid Wise Architecture Council (GWAC). An eight-layer stack, termed the GWAC stack, provides a context for determining smart grid interoperability requirements and defining exchanges of information.

The layers represent the chronological processes that enable various interactions and transactions within the smart grid. Each layer depends upon the layer beneath it and so each layer must function properly for the entire stack to be effective. As more complex functions are required by the network, more layers will be required to achieve interoperability. According to GWAC, each category/driver subdivided by layers has a special purpose, as follows:

- Technical: Emphasizes the syntax or format of the information, focusing on how the information is represented on the communication medium
- Informational: Emphasizes the semantic aspects of interoperation, paying attention to what information is exchanged and its meaning
- Operational: Emphasizes the pragmatic (business and policy) aspects of interoperation, especially those pertaining to the management of electricity

5.2.4 Smart Grid Network Interoperability

Machines require specific data and instructions to complete tasks. The challenge is to design language and protocols to ensure effective communication between machines that are governed by the same protocol and even more so for those using different protocols. The main issue is to facilitate efficient, quick, and speedy transfer of data among and across devices. Interoperability is not limited to a physical aspect of the network, since design engineers must also consider that

as two devices try to exchange data, the messages must now “speak the language” of network navigation and be properly “addressed” to reach the destination device.

This issue creates the need for networking standards so that machines that need to be connected can communicate without interruption or disruption. Unfortunately, this is not a simple task to undertake. For example, some machines may use a particular language protocol that requires another machine attempting to communicate to complete specific system requirements, which may be outside its scope, before transmission can be completed. In this case, the data transfer/communication may be prohibited or incomplete, making the network inefficient.

5.2.5 Interoperability and Control of the Power Grid

As discussed in the previous section, network control is a major issue for utilities. To upgrade to a smart system, the network should be outfitted with equipment that can detect problems, report back to the utility, receive control or restorative commands, and execute them. Full control will require that all machines communicate, interpret, and perform tasks that most machines today cannot do.

The use of SCADA and EMS have become ineffective, and leaves control centers with the need to communicate with other control centers as well as regulatory agencies, energy markets, independent power producers, large customers and suppliers, to keep up with the evolving market environment . Control centers must be able to connect to machines that have smart technology to facilitate effective performance with little or no interruptions. Ultimately, the user/customer should have some degree of autonomy over consumption with a faster, more effective response to supply disruptions

5.3 STANDARDS

Standards are the specifications that establish the fitness of a product for a particular use or that define the function and performance of a device or system. Many standards bodies, including the National Institute of Standards and Technology (NIST), International Electro technical Commission (IEC), Institute of Electrical and Electronic Engineers (IEEE), Internet Engineering Task Force (IETF), American National Standards Institute (ANSI), North American Reliability Corporation (NERC), and the World Wide Web Consortium (W^3C) are addressing interoperability issues for a broad range of industries, including the power industry.

The urgent need for the development of standards has led NIST to develop a plan to accelerate the identification and establishment of standards “while establishing a robust framework for the

longer term evolution of the standards and establishment of testing and cortication procedures." Based on the first phase of this work, NIST published the NIST Framework and Roadmap for Smart Grid Interoperability Standards Release 1.0 in September 2009 .In this publication, nearly 80 existing standards are identified.

5.3.1 Approach to Smart Grid Interoperability Standards

The roadmap for interoperability by NIST includes the following applications:

- Demand Response and Consumer Energy Efficiency
- Wide Area Situational Awareness
- Electric Storage
- Electric Transportation
- Advanced Metering Management
- Distribution Grid Management
- Cyber Security
- Network Communications
- These standards are applicable to transmission and/or distribution systems and pertain to electrical power system components.
- Additionally, there are several standards identified for different levels of communication, demand response, and measurement devices. As an example, in the area of power quality, the IEEE and other governing bodies have their own sets of standards.

5.4 SMART GRID CYBER SECURITY

Cyber security is a concept that has become increasingly prevalent with the development of the smart grid technology with the increased use of digital information and controls technology to improve reliability, security, efficiency of the electric grid and the deployment of smart technologies (real-time, automated, interactive technologies that optimize the physical operation of appliances and consumer devices) for metering, communications concerning grid operations and status, and distribution automation. The interaction of the power, communication, and information networks are critical to facilitating resiliency and sustainability of the infrastructures which further enhance the provision of adequate power and support economic and social growth of the nation. Technologies and protocols are developed for the maintenance of system, network, data, and SCADA security while conducting vulnerability assessment, incident recognition, recording, reporting, and recovery. Protection of network data as well as web-based or stored data is conducted.

5.4.1 Cyber Security State of the Art

Cyber security is a critical priority of smart grid development. However, the cyber security requirements for the smart grid are in a considerable state of flux. Cyber security includes measures to ensure the confidentiality, integrity, and availability of the electronic information communication systems necessary for the management and protection of the smart grid's energy, information technology, and telecommunications infrastructure.

This infrastructure includes information and communications systems and services and the information contained in these systems and services. Information and communications systems and services are comprised of the hardware and software that process, store, and communicate information, or any combination of all of these elements. Processing includes paper, magnetic, electronic, and all other media types.

Cyber security is defined as security from threats conveyed by computer or com- puter terminals and the protection of other physical assets from modification or damage from accidental or malicious misuse of computer-based control facilities. Smart grid security protocols contain elements of deterrence, prevention, detection, response, and mitigation; a mature smart grid will be capable of thwarting multiple, coordinated attacks over a span of time. Enhanced security will reduce the impact of abnormal events on grid stability and integrity, ensuring the safety of society and the economy.

There is a cyber security coordination task force directed at the design of grid security at the architectural level. Tasks include identifying used case studies with cyber security considerations, performing risk assessment such as vulnerabilities, threats and impacts as well as developing security architecture.

The underlying concept is that security should be built-in, not added-on. This strategy includes:

- Review of the system functionality and data flows with particular attention to their similarities and differences with identified smart grid use cases (as documented in the NIST Roadmap).
- Identification of relevant threats and the consequences/impacts if the confidentiality, integrity, availability, or accountability of the system data flows are compromised.

Security requires many different solutions and is not relegated to encryption and password protection. Facets of the cyber security include:

- Security assessment and hardening of the existing systems

- Vulnerability assessment
- Disaster recovery
- Intrusion detection incident response
- Event logging, aggregation, and correlation

Another critical understanding of the issue of security for the purpose of development is the realization of the inevitability of the occurrence of breaches. This leads to the development of contingency and recovery plans.

Critical objectives for the development of cyber security for the smart grid environment are ensuring the confidentiality, integrity, and availability of device and system data and communications channels, and securing logging, monitoring, alarming, and notification. Data protection will require confidentiality of communicated and stored data for the power system facilitated by authentication methods and the use of cryptography which includes encrypted authentication, to make it difficult for hackers. A combination of detective, corrective, and preventive controls will address cyber security risks. As the risks are determined, the best approach will balance efficiency, cost, and effectiveness.

All known cyber threats are monitored with a form of detective control. These include technologies such as host-based intrusion detection systems (HIDS) to monitor unauthorized changes to servers and deployed systems, network-based intrusion detec- tion systems (NIDS) to detect network-based attacks, and platform-specific controls like virus detection and malware detection. These detective controls provide vital data to design and testing staff about the real attacks and threats that the system faces. Detective controls often provide forensic-quality evidence that can be used to reconstruct attacks and potentially identify and/or prosecute attackers. Additionally, data from detective controls also assist in the selection of corrective and preventive controls.

Corrective controls seek to restore normal operations in the event of a successful cyber attack. Such controls are both manual, for example, a standardized procedure for switching to a backup system, and automatic, for example, failover designs that automatically disable compromised systems and replace them with known good systems. Corrections often seek to isolate and preserve successful attacks so that forensic analysis can proceed and permanent corrections, for example, in design, construction, or deployment, can be established.

For example, the secure development approach seeks to address risk throughout the life-cycle and throughout the engineering process, but preventive controls are a logical, efficient, and effective complement to secure implementation. Some attacks, for example, denial-of-service, can only be mitigated with a combination of secure engineering and preventive controls. Other attacks can be partially mitigated with a protective control, for example, network rules or role-based access controls, until a more comprehensive change to the system can be developed, tested, and deployed. As required, Grid Point deploys preventive controls to satisfy regulations, adhere to best practices, or to mitigate cyber security risks, including network-level filtering and rules, operating system-level mechanisms, and hardware-level mechanisms

5.4.2 Cyber Security Risks

Cyber security risks appear in each phase of the project life-cycle and include risks to managerial, operational, and technical processes. These risks may impact equipment and systems, network management and integration, communications, control and opera- tions, and system availability. The primary components that may be vulnerable to security risks include IT applications, communications network, and endpoints (for example, meters, in-home displays, and thermostats). There are substantial risks to the integrity of data and control commands due to the exchange of information through publicly accessible equipment, for example, smart meters using over-the-air communi- cations technologies, for example, wireless or radio frequency, which may be intercepted and altered if not appropriately secured.

A number of system constraints need to be taken into account when satisfying security requirements. The requirements described do not prescribe which solution, for example, the use of narrow- or wide-band communications technologies, is most appropriate in a given setting. Such a decision is typically based on making prudent trade-offs among a collection of competing concerns. The following trade-off must include the considering cyber security risk:

- Other business or non-functional requirements
- Performance (for example, response time)
- Usability (for example, complexity of interactions for users)
- Upgradability (for example, ease of component replacement)
- Adaptability (for example, ease of reconfiguration for use in other applications)
- Effectiveness (for example, information relevant and pertinent to the business process as well as being delivered in a timely, correct, consistent, and usable manner)
- Efficiency (for example, the provision of information through the most productive and economical use of resources)

- Confidentiality (for example, protection of sensitive information from unauthorized disclosure)
- Integrity (for example, accuracy, completeness, and validity of information in accordance with business values and expectations)
- Availability (for example, information being available when required by the business process)
- Compliance (for example, complying with the laws, regulations, and contractual arrangements)
- Reliability (for example, the provision of appropriate information for management to operate the entity and exercise its fiduciary and governance responsibilities)

It is important to consider system constraints when developing applying security requirements, which include:

- Constraints
- Computational (for example, available computing power in remote devices)
- Networking (for example, bandwidth, throughput, or latency)
- Storage (for example, required capacity for firmware or audit logs)
- Power (for example, available power in remote devices)
- Personnel (for example, impact on time spent on average maintenance)
- Financial (for example, cost of bulk devices)
- Temporal (for example, rate case limitations)
- Technology
- Availability
- Maturity
- Integration/Interoperability (for example, legacy grid)
- Life-cycle
- Interconnectedness of infrastructure
- Applications (for example, automated user systems and manual procedures that process the information)
- Information (for example, data, input, processed and output by the information systems in whatever form is used by the business)
- Infrastructure (for example, technology and facilities, that is, hardware, operating systems, database management systems, networking, multimedia, and the environment that houses and supports them, that enable processing the applications)

- People (e.g., the personnel required to plan, organize, acquire, implement, deliver, support, monitor, and evaluate the information systems and services. They may be internal, outsourced or contracted as required) will consider: time, financial, technical, operational, cultural, ethical, environmental, legal, ease of use, regulatory requirements, scope/sphere of influence

5.4.3 Cyber Security concerns Associated with AMI

AMI is the convergence of the power grid, the communications infrastructure, and the supporting information infrastructure. This system of systems is constituted by a collection of software, hardware, operators, and information and has applications to billing, customer service and support, and electrical distribution.

The development of the security domain for AMI systems and a security domain model was developed to bound the complexity of specifying the security required to implement a robust, secure AMI solution and to guide utilities in applying the security requirements to their AMI implementation. Each utility's AMI implementation will vary based on the specific technologies selected, the policies of the utility, and the deployment environment.

5.4.4 Mitigation Approach to Cyber Security Risks

This process of mitigation of errors or sources of insecurity includes the following:

- Identifying and classifying the information that needs to be protected
- Defining detailed security requirements
- Reviewing the proposed security architecture that is designed to meet the requirements
- Procuring a system that is designed to meet the specified security requirements and includes the capability to be upgraded to meet evolving security standards
- Testing the security controls during the test and installation phase
- Obtaining an independent assessment of the security posture before deployment
- Developing a remediation plan to mitigate the risks for identified vulnerabilities
- Installing a system with built-in management, operational, and security controls
- Monitoring and periodically assessing the effectiveness of security controls
- Migrating to appropriate security upgrades as security standards and products mature
- Monitoring of communication channels
- Monitoring spike in usage (meter reading) to detect possible failures or tampering

with the devices

- Making sure devices synchronize with the network within a given time frame to detect tampering, potential problems, and device failures.
- Penetration testing will be performed using the latest hacking techniques, to attempt to break into the systems, identifying possible vulnerabilities, and remotely validating the authenticity of the software running in the meters.

5.5 Cyber Security and Possible Operation For ImprovingMethodology For Other Users

Every communication path that supports monitoring and control of the smart grid is a two-way communication path. Each path is a potential attack path for a knowledgeable attacker. There are many potential entry points physically unprotected. Wireless net- works can be easily monitored by attackers and may be susceptible to man-in-the- middle (MitM) attacks. Security mechanisms in place are intended to prevent unauthorized use of these communication paths, but there are weaknesses in these mechanisms. The history of security in complex networks implies that more vulnerability is yet to be discovered.

Thus, the key points include:

1. Using spot checks on systems to go beyond the current paper chase approach to validating CIP compliance
2. Acknowledging that attackers and malware will find ways around/through current outer-wall–based network defenses, instituting a less-perimeter, defense- oriented approach to security controls with guidance on use of DMZs between internal networks.

5.6 Case Study Of RER Integration

1. AEP, which has its own existing EHV 765 kilovolt (kV) network, consisting of 19,000 miles of transmission lines, would establish a combined additional capacity of perhaps 200–400 GW of bulk transmission, thus spurring significantly increased levels of wind energy in the overall energy portfolio. AEP estimated the cost in the range of $60 billion in 2007.
2. Cape Wind took one step closer to becoming the first offshore wind producer in the United States when Massachusetts regulators approved a power purchase agreement with National Grid for fifty percent of the output. The state's Supreme Judicial Court is expected to rule on the PPA by December 31, 2011.
3. Southern California Edison is moving toward smaller PV plants as the price of solar

panels continues to drop. It recently signed contracts for 239.5 MW to be provided by 20 small solar farms.

4. A U.K.-based electricity company is developing an electric sports car that gets its power from wind turbines, to break the British land speed record of 139 mph in 2012.
5. With 45 wave and tidal prototypes slated for ocean testing this year and next, IHS Emerging Energy Research says the global ocean power market looks poised for takeoff.
6. The U.S. Navy is planning to roll out about 10 ships, planes and submarines powered by a blend of biofuels and nuclear power.

5.6.1 Description of Smart Grid Activity

Two important ways that smart grid technology creates value in the transmission network are

- Direct interconnection of large-scale resources
- Using remote sensing (and eventually, remote devices for the injection of dynamic reactive power) to increase network capacity by improving flow management

5.6.2 Approach for Smart Grid Application

Advanced metering infrastructure (AMI). AMI is a catch-all term for smart meters. The smart grid is often associated with electrical meters, or smart meters. This association helps to simplify a very complex process, but it sells the vision of the smart grid short.

The smart grid is no more about the meter than the economy is only about the cash register. Both are merely collection points: interfaces between buyer and seller where data can be gathered and analyses. As in many business and technology scenarios, you can't improve what you can't measure. AMI systems capture data, typically at the meter, to provide information to utilities and transparency to consumers. It's also usually the case that AMI systems piggyback on a variety of wireless systems. One simple illustration: the days of the electric company representative swinging by to read your meter could be phased out with AMI.

Demand response (DR). To date, consumers have used energy whenever they want to, and utilities have built the power plants and delivery infrastructure to support it, no matter what the cost or environmental impacts. To achieve economic and environmental goals, consumers need to become equal participants in the process, tuning their energy consumption to when clean resources are available and avoiding peak energy consumption times as much as they can. If some electricity-consuming devices can be deferred to nonpeak time, everyone wins. While you

may need to turn on your lights when you arrive home, there's no reason that you can't run your dishwasher at 3 AM when rates and demand are lower.

That's the reasoning behind demand response programs and they have been very successful. Research bears out again and again that when consumers are asked to "do the right thing" when it comes to energy usage, they will do so.

Smart thermostats, for example, can prompt consumers to lower their air conditioner by a degree or two. To date, some U.S. citizens are in some kind of demand response program. In-home displays and similar devices can lower energy use by up to 6%. Demand response programs yield immediate reductions on the average.

Critical peak pricing (CPP). An off-shoot of demand response, critical peak pricing simply means that utilities have the technology infrastructure in place to charge consumers more for energy during peak periods. It allows customers to decide whether or not to pay more on the specific critical days, rather than paying an average cost. It helps balance cost and risk between the consumer and the utility, as well as providing a further incentive for consumers to reduce energy consumption.

Time-of-Use Pricing (TOU). Time-of-use pricing is similar to critical peak pricing, except extrapolated across every hour for every day. Time-of-use pricing allows utility rates and charges to be assessed based on when the electricity was used. Not only the time of day, but also the season, as well as accounting for local weather pat- terns that might prompt a rate adjustment (at which point it becomes a demand response application).

Short and Long Answer Type Questions

1. Define interoperability in Smart Grid environment.
2. Explain the concept of interoperability in Smart Grid.
3. Brief on smart grid interoperability standards.
4. Write a short notes on
    i. Cyber Security Risk
    ii. Mitigation Approach to Cyber Security Risks
5. Why cyber security required for smart grid and how it's adopted?
6. Brief on Cyber security concerns associated with AMI.
7. Explain the case study in smart grid activity and approach for smart grid application.
8. Write short on Demand response (DR).
9. Define the following terms:
    i. Critical peak pricing (CPP)
    ii. Time-of-Use Pricing (TOU)

.

A Text Book on

Smart Grid Technology

Dr. K. Saravanan is a professor and Head of Department of Electrical and Electronics Engineering. Dr. MGR Educational and Research Institute Chennai. He has 25 years of Teaching and Research Experience. He has published several Research papers in journals and conference both National and international. He obtained B.E from the Government College of Technology Coimbatore. M.E and Ph.D. from Anna University Chennai. He has been involved in Teaching and Research in the area of Power electronics, Electrical Machines, and Hybrid Renewable Energy systems he has been involved in several research development and laboratory modernization projects. He has also worked as a consultant in the area of rice mill boiler heat exchanger.

Er. A. Raja Currently Working as Assistant Professor in Department of Electrical and Electronics Engineering in Dr. MGR Educational and Research Institute, Chennai, Tamilnadu, India. He completed his B.E (EEE) and M.E (Power systems Engineering)during the year 1996 and 2005 respectively. His area of interest includes Smart grid technologies, Optimal power flow. He has total teaching experience of 20 years. He has published many papers in International Journals and conferences.

Dr. R. Sivanand Currently Working as Assistant Professor in Department of Electrical and Electronics Engineering in Dr. MGR Educational and Research Institute, Chennai, Tamilnadu, India., holds Ph.D. Degree. He has 19 Years of Experience in the Teaching, his area of interests includes Electrical Machines, Control System, Power Electronics, Renewable Energy, Nanomaterials etc.,

Dr. K. Senthilkumar, working as Professor in Electronics & Communication Department, Dr. M.G.R Educational and Research Institute University, Chennai. He has more than 22 years of experience in Educational Institute. His Field of Specialization is VLSI Design, Single Electron Transistor and Nano Devices. He has published more than 55 Papers in National & International Journals. He is recognized Supervisor, guiding Ph.D. Scholars who have registered in Dr. M.G.R Educational and Research Institute, University, Chennai.

9 789395 054539